Microsoft Azure

Ensure well-governed & Secure Azure environments

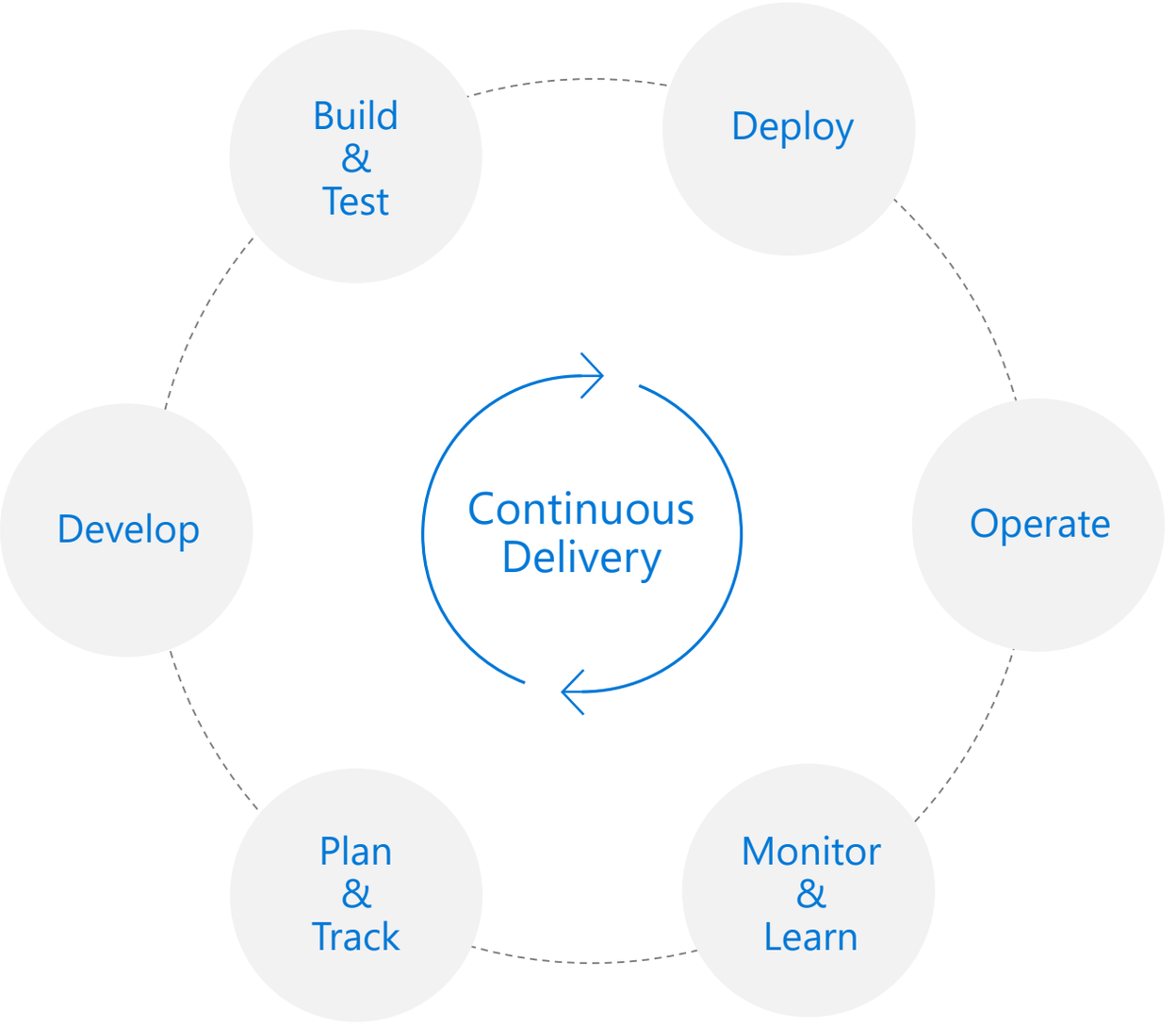
Joe Losinski

Partner Technology Strategist

What is DevOps?

People. Process. Products.

> DevOps is the union of **people**, **process**, and **products** to enable continuous delivery of value to your end users.

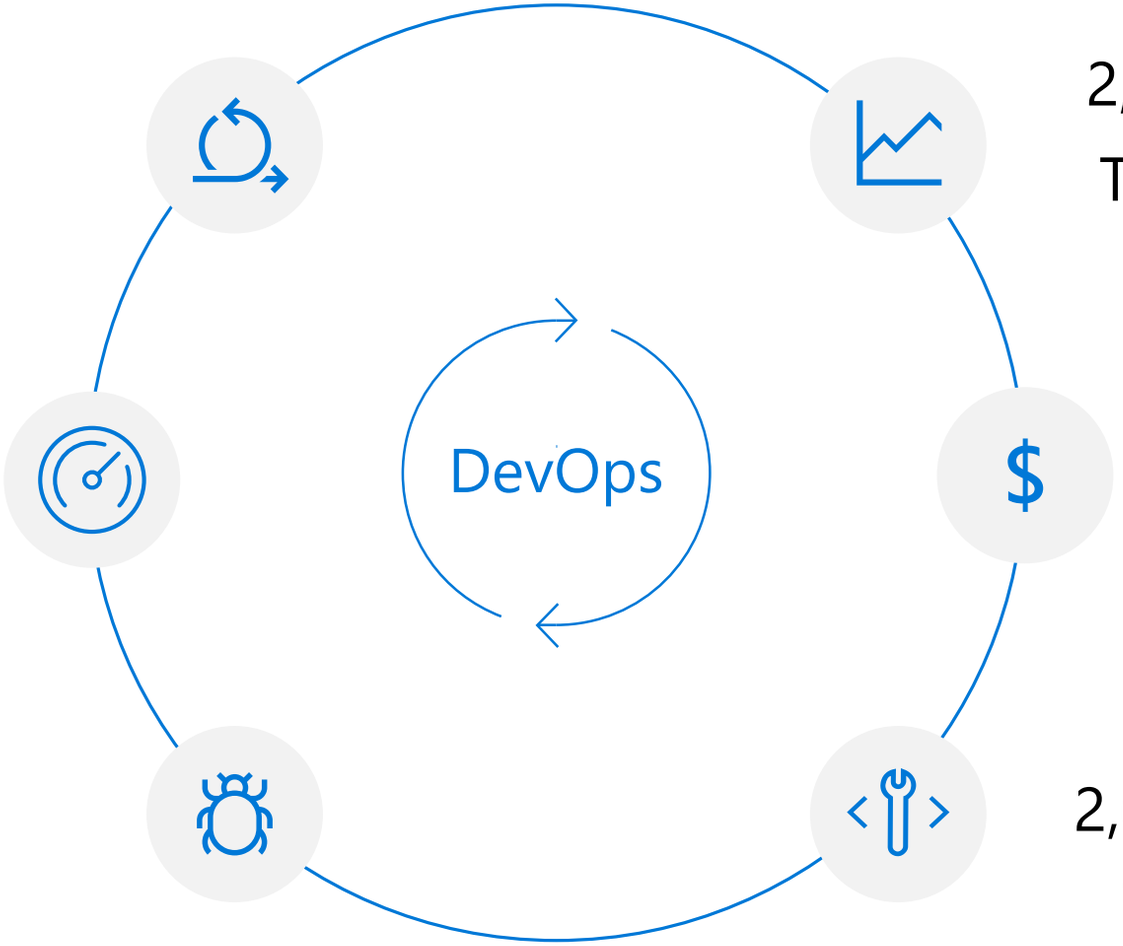


High Performance DevOps Companies Achieve…

46x Deployment Frequency

Faster Time to Market

7x Lower Change Failure Rate



2,555x Faster Lead Time For Changes

Increased Revenue

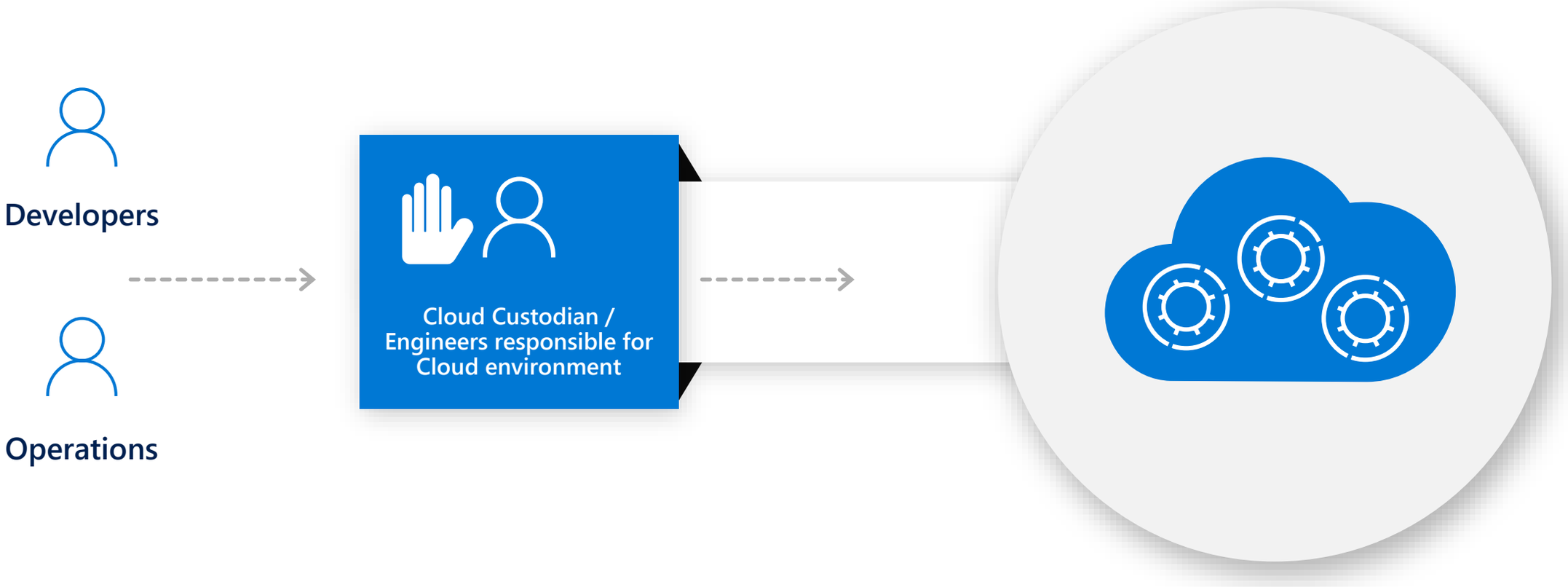
2,604x Faster Mean Time to Recover

Source: 2018 Accelerate: State of DevOps: Strategies for a New Economy." N. Forsgren, J. Humble, G. Kim. DevOps Research and Assessment (DORA)

Governance, Risk, & Compliance

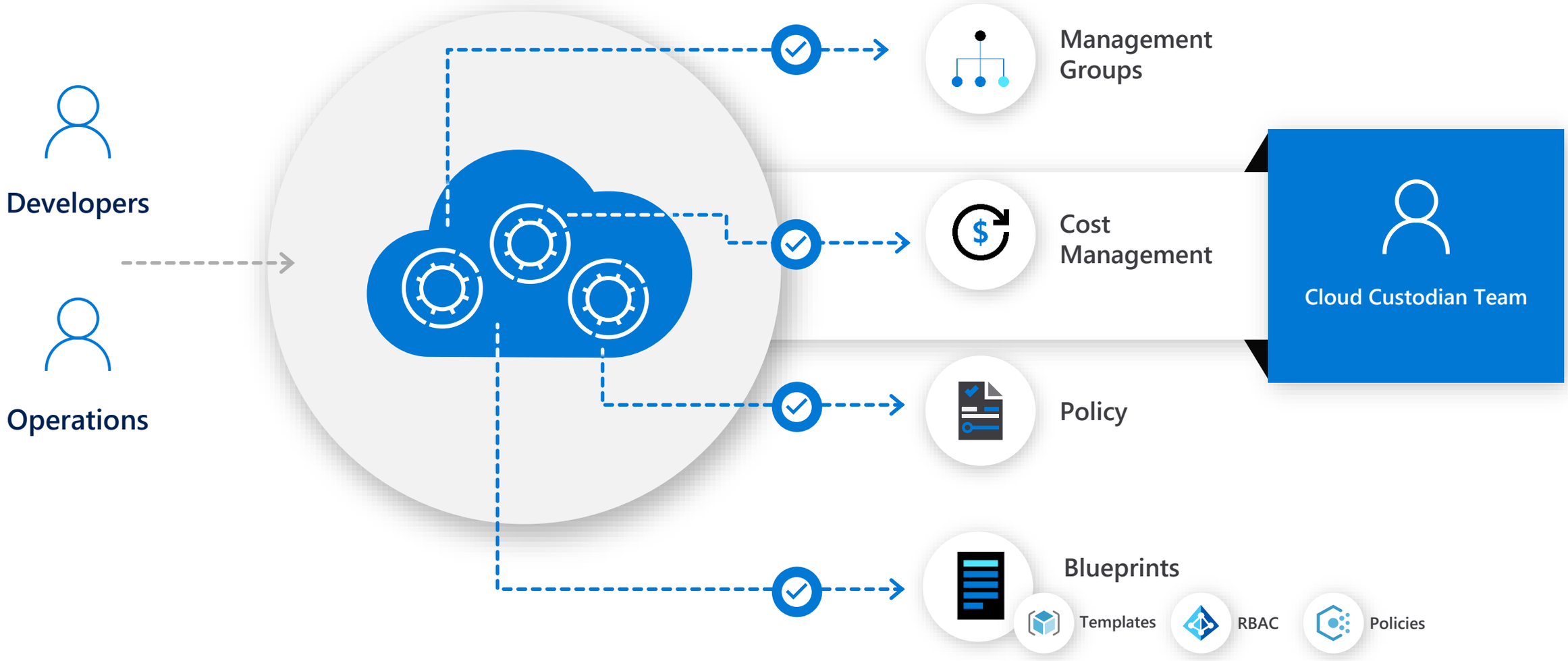
Traditional approach

Block Dev/Ops from directly accessing the cloud (portal/api/cli) to attain control



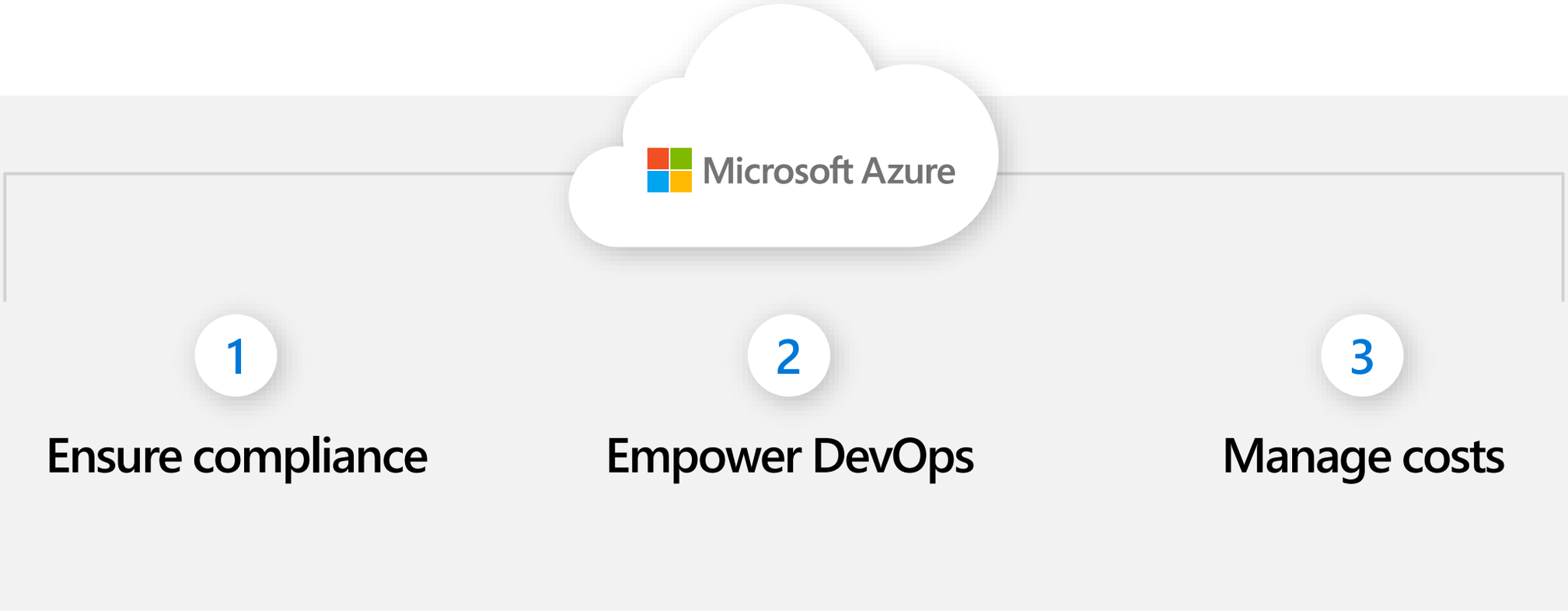
Speed + Control

Cloud-native governance -> removing barriers to compliance and enabling velocity



Azure is designed for effective governance

Enforce compliance at scale and increase agility



Governance for the cloud

The broadest governance portfolio of any cloud

Management Group

Define organizational hierarchy

Hierarchy

Policy

Real-time enforcement, compliance assessment and remediation

Control

Blueprints

Deploy and update cloud environments in a repeatable manner using composable artifacts

Environment

Resource Graph

Query, explore & analyze cloud resources at scale

Visibility

NEW

Cost Management

Monitor cloud spend and optimize resources

Consumption

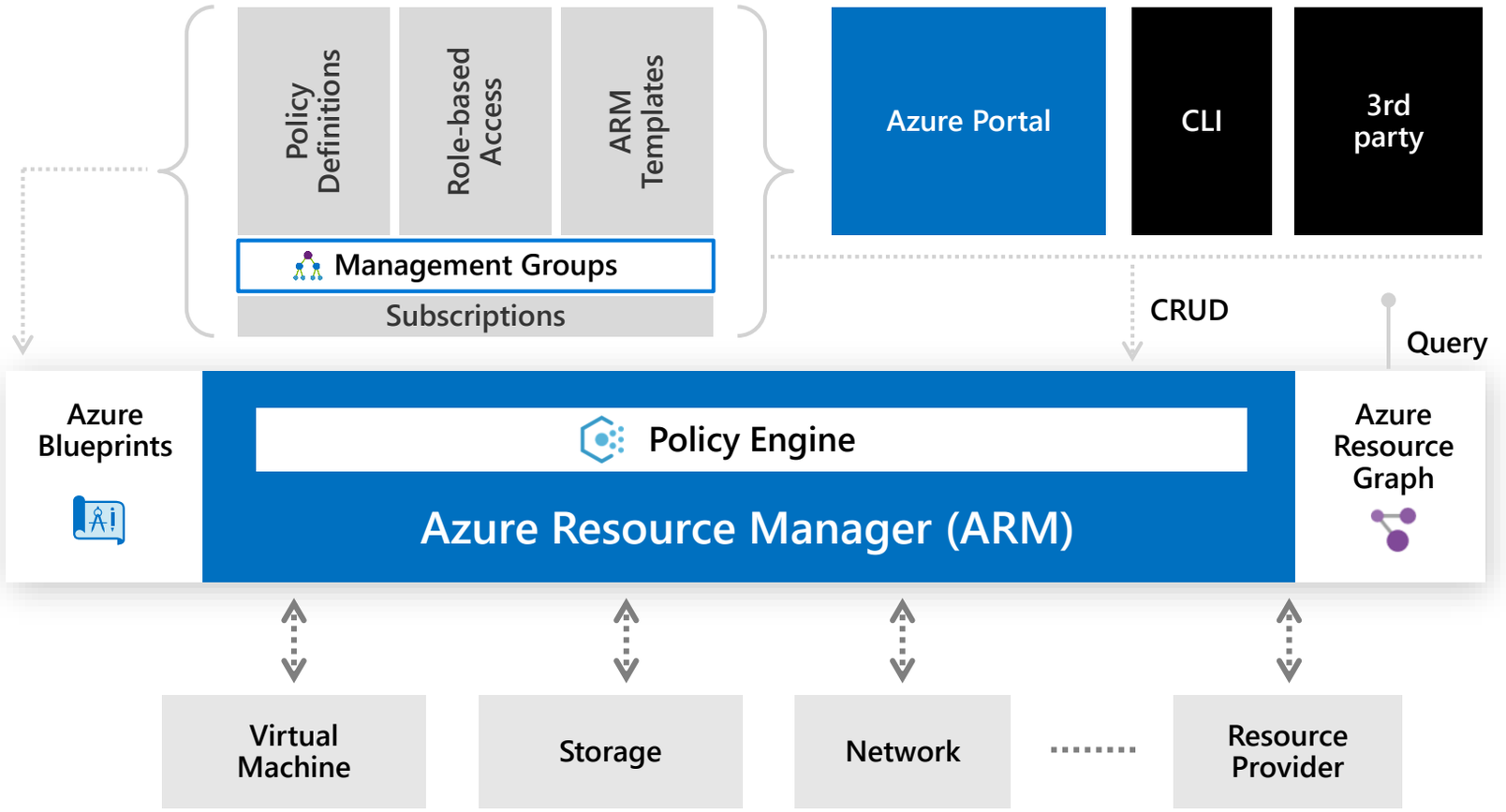
Azure Governance Architecture

Providing control over the cloud environment, without sacrificing developer agility

1. **Environment factory**
   Deploy and update cloud environments in a repeatable manner using composable artifacts

2. **Policy-based control**
   Real-time enforcement, compliance assessment and remediation at scale

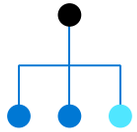
3. **Resource visibility**
   Query, explore & analyze cloud resources at scale



Introducing Azure Management Groups

Efficiently apply governance controls and manage groups of Azure subscriptions

1. Ensure compliance
2. Empower DevOps
3. Manage costs

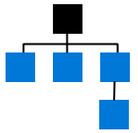


Simplify subscription management

Group subscriptions into logical groups

Inherit properties that apply to all subscriptions

View aggregated information above the subscription level

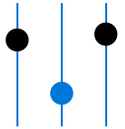


Fit your organization

Create a flexible hierarchy that can be updated quickly

Mirror the hierarchy to the organizational model that works for you

Scale up or down depending on the organizational needs



Apply controls at scale

Leverage Azure Resource Manager (ARM) objects that integrate with other Azure services

Azure services:

Azure Policy

RBAC

Azure Cost Management

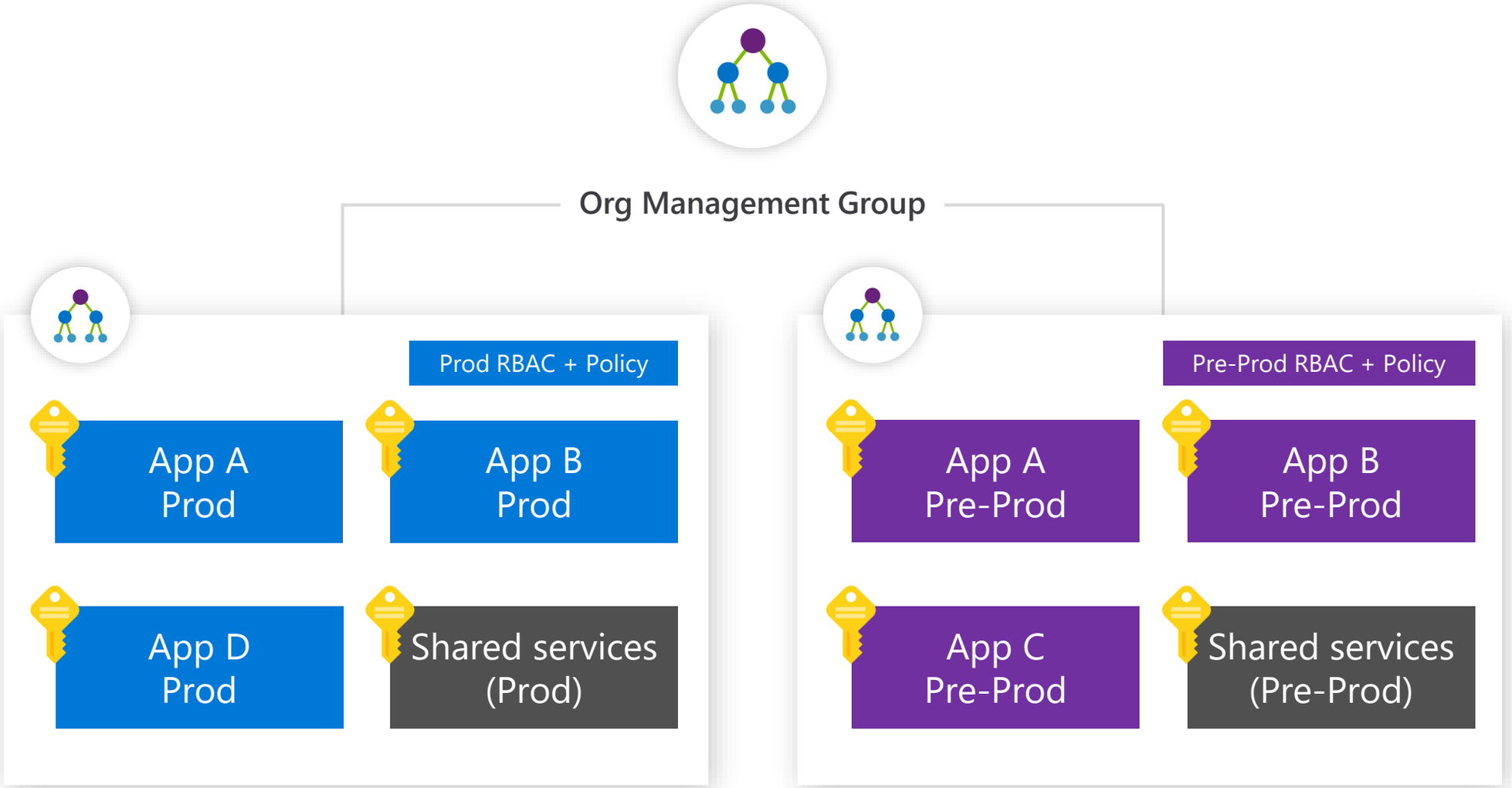
Azure Blueprints

Azure Security Center

Management Group & subscription modeling strategy

1. Ensure compliance
2. Empower DevOps
3. Manage costs

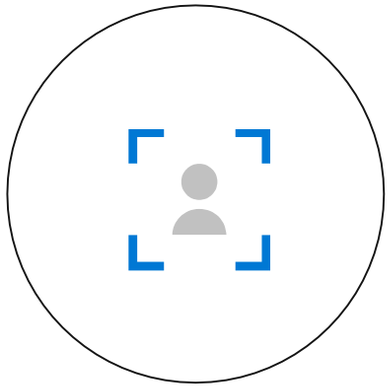
Microsoft recommended



Introducing Azure AD Identity Governance

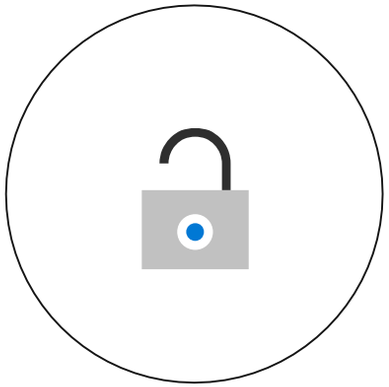
1. Ensure compliance
2. Empower DevOps
3. Manage costs

MFA



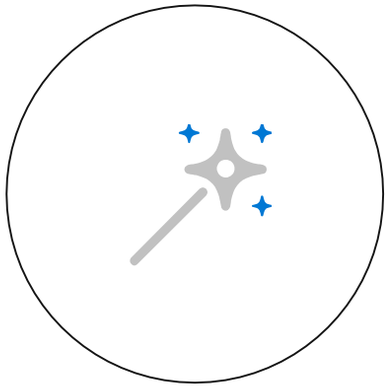
Identity lifecycle
facilities collaboration

Conditional Access



Access lifecycle
provides seamless and efficient access

Privileged Identity Management



Privileged access lifecycle
addresses risks inherent in administration

RBAC (Role Based Access Control)

Ensure the **right users** have the **right access** to the **right resources**

Azure Policy

Active control and governance at scale for your Azure resources

1 Ensure compliance

2 Empower DevOps

3 Manage costs

Enforcement & compliance

Turn on built-in policies or build custom ones for all resource types

Real-time policy evaluation and enforcement

Periodic & on-demand compliance evaluation

VM In-Guest Policy (**NEW**)

Apply policies at scale

Apply policies to a Management Group with control across your entire organization

Apply multiple policies and & aggregate policy states with policy initiatives

Exclusion Scope

Remediate & automate

Remediate existing resources at scale (**NEW**)

Automatic remediation resources at deployment time

Trigger alerts when a resource is out of compliance

Enforce policies as part of the development process

Shift left to deliver compliant code faster

1. Ensure compliance
2. Empower DevOps
3. Manage costs

Code | Build/Test | Deploy | Operate

Policy as Code

Pre-flight

Validation

Authoring

Policy

Security

Monitoring

Azure DevOps

Enforce policies as part of the development process

Shift left to deliver compliant code faster

1 Ensure compliance

2 Empower DevOps

3 Manage costs

Code | Build/Test | Policy as Code: Pre-flight / Validation / Authoring | Deploy | Operate

Policy

Security

Monitoring

Azure DevOps

Azure Policy

Azure Blueprints

Enabling quick, repeatable creation of fully governed environments

1. Ensure compliance
2. Empower DevOps
3. Manage costs

Streamline environment creation

Centralize environment creation through templates

Add resources, policies and role access controls

Track blueprint updates through versioning

Enable compliant development

Empower developers to create fully governed environments through self-service

Create multiple dev-ready environments and subscriptions from a centralize location

Leverage the integration with Azure Policy on the DevOps lifecycle

Lock foundational resources

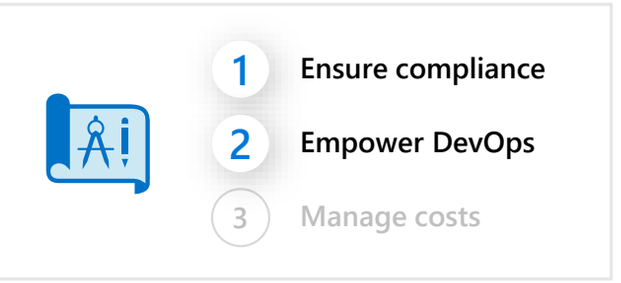
Ensure foundational resources cannot be changed by subscription owners

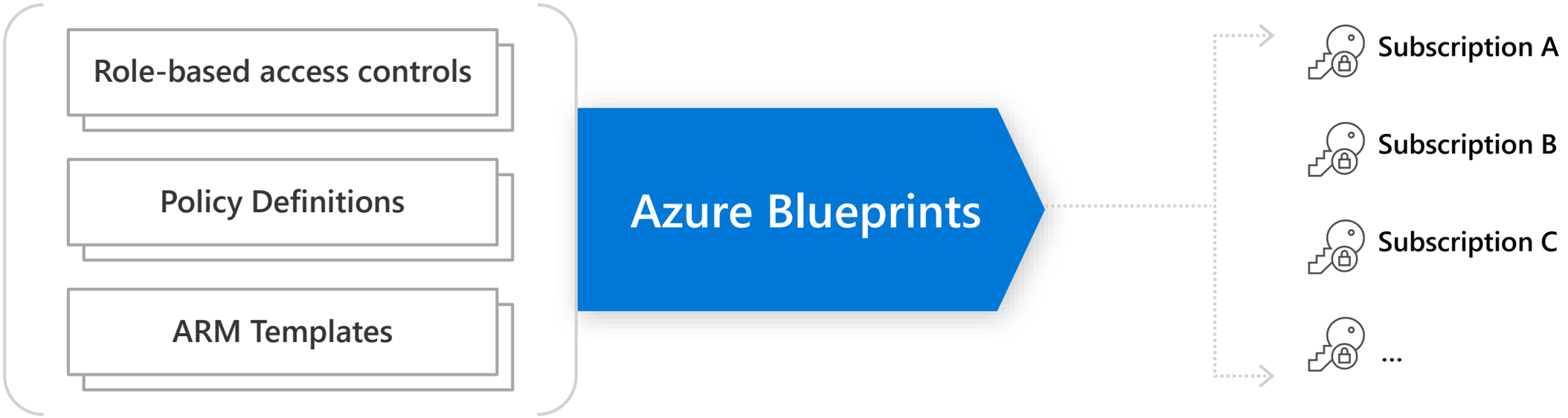
Manage locks through a centralize location

Update locked resource through blueprint definition updates

Azure Blueprints

deploy and update cloud environments in a repeatable manner using composable artifacts





Compose | Manage | Scale

Faster development cycles through Blueprints

Microsoft Core Services Engineering

“Azure Blueprint's allows our central IT to ensure the right guardrails are in place helping our DevOps teams move fast while maintaining control/protecting the business."

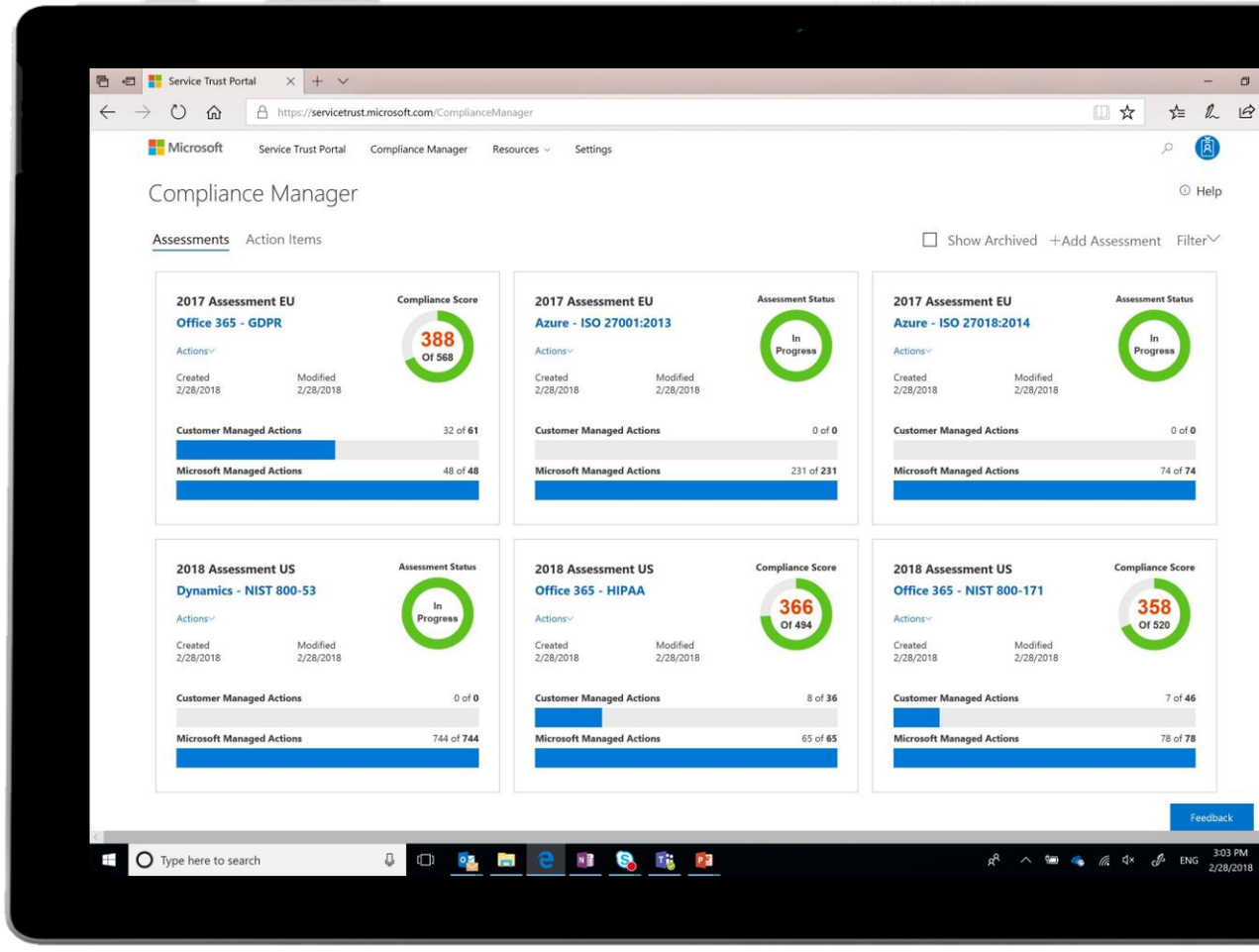
— **Pete Apple**
Lead Service Engineer

Compliance Manager

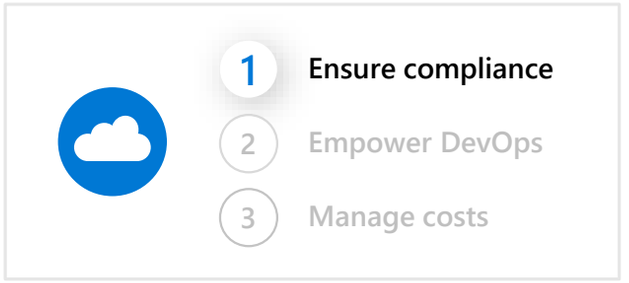
A single pane of glass

1. Ensure compliance
2. Empower DevOps
3. Manage costs

- **Ongoing Risk Assessment**
  An intelligent score reflects your compliance posture against regulations or standards.
- **Compliance Score**
- **Summary of data protection and compliance stature**
- **Recommendations to improve data protection and compliance**



Caveats for using Compliance Manager



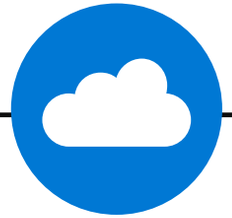
Recommendations from Compliance Manager and Compliance Score **should not be interpreted as a guarantee of compliance.**

Compliance Manager gives you tools and information to perform **self-assessment** of the controls you manage.

You are responsible for evaluating and validating the effectiveness of your controls relative to your regulatory environment.

Current availability of Compliance Manager

1 Ensure compliance
2 Empower DevOps
3 Manage costs



CLOUD SERVICES

Office 365
Microsoft Azure
Microsoft Dynamics 365

REGULATIONS AND STANDARDS

NIST National Institute of Standards and Technology U.S. Department of Commerce **800-171**

NIST National Institute of Standards and Technology U.S. Department of Commerce **800-53**

GDPR

Information Security Management System ISO 27001

Information Security Management System ISO 27018

HIPAA Health Insurance Portability & Accountability Act

**Coverage of regulations and standards in Compliance Manager varies by product. We will keep adding and updating the information in the future and our goal is to provide similar experience of using Compliance Manager for all Microsoft Cloud services.*

Azure Resource Graph

Get visibility into your resources for effective inventory management

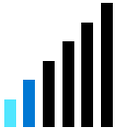
1. Ensure compliance
2. Empower DevOps
3. Manage costs

Explore your resources

Get visibility into your Azure resources across subscriptions and management groups.

Access the information you need in the portal, CLI or PowerShell

Find assets based on resource properties or their relationships



Query & analyze

Get the exact information you need through queries in seconds

Perform analysis at scale across all your environments

Leverage Keyword Query Language for easy query creation

Assess impact

Understand the impact of applying policies before their implementation

Get a view of the operational impact of common actions like deprecations

Azure Cost Management

1 Ensure compliance

2 Empower DevOps

3 Manage costs

Monitor cloud spend

Track usage and cost trends

Detect spending anomalies and usage inefficiencies

Forecast future spend using your historical data

Visualize data in consolidated or custom dashboards

Drive organizational accountability

Allocate usage and costs to business units and projects

Produce chargeback and show back reports

Let teams access data and insights with Role-Based Access Control

Automatically alert stakeholders of spending anomalies and overspending risks

Optimize cloud efficiency

Increase resource utilization with virtual machine right-sizing

Eliminate idle resources

Improve virtual machine reserved instances management

Pay less for Windows Server and SQL Server resources through Azure Hybrid Benefit

Azure Cost Management

1. Ensure compliance
2. Empower DevOps
3. Manage costs

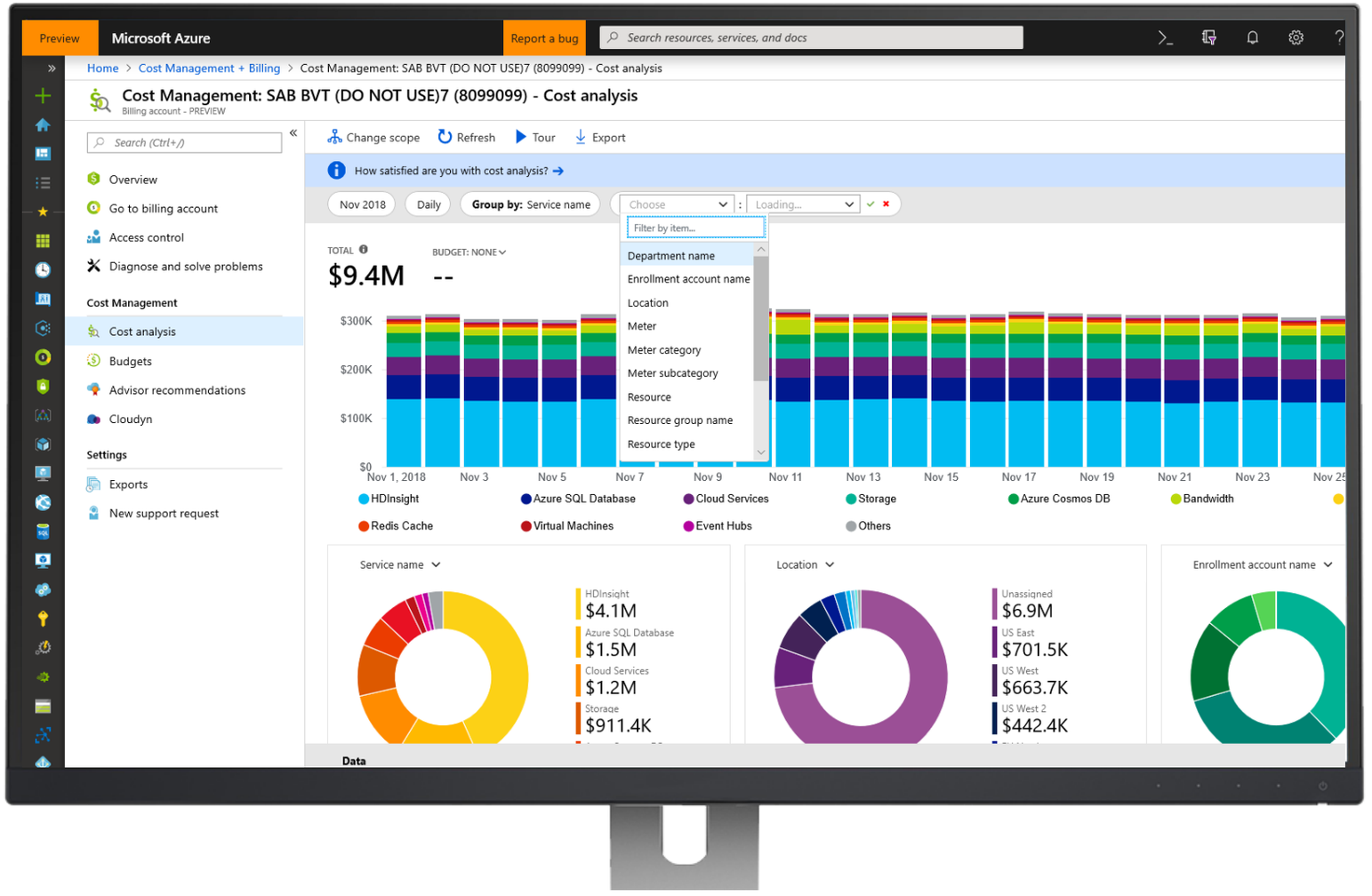
Monitor cloud spend

Track usage and cost trends

Detect spending anomalies and usage inefficiencies

Forecast future spend using your historical data (Coming soon)

Visualize data in consolidated or custom dashboards



Azure Cost Management

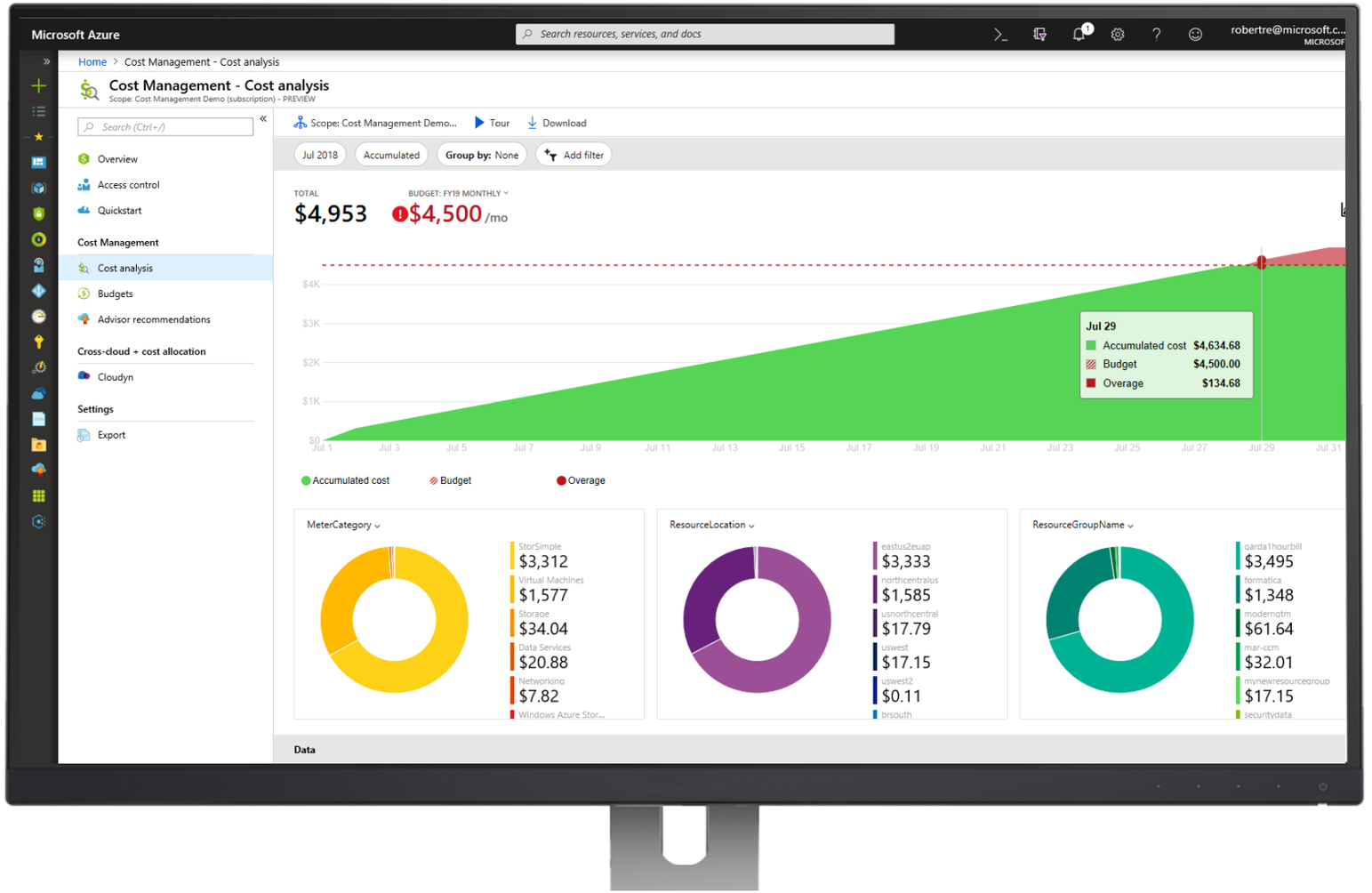
1 Ensure compliance
2 Empower DevOps
3 Manage costs

Drive organizational accountability

Ability to create budgets and alerts

Let teams access data and insights with Role-Based Access Control

Automatically alert stakeholders of spending anomalies and overspending risks




Azure Lighthouse

> The ethos of being partner led is always going to be in everything we do.

Satya Nadella
Inspire 2017

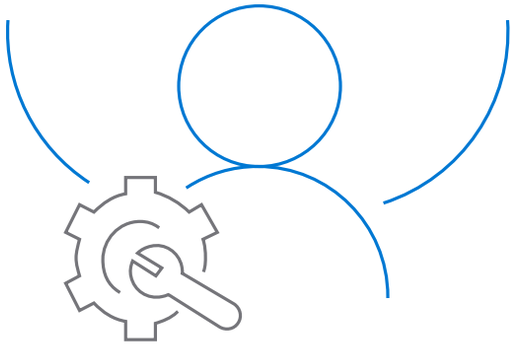
We are at an inflection point, recognizing the need to nurture our partner ecosystem and extend automation & scalability across scenarios

Individual customer management

Stitching third-party tools with scripting

Customers in regulated markets with strong compliance policies

Access that does not lend itself to automation



Azure Lighthouse

Enabling partners to deliver differentiated managed services

Azure Lighthouse provides capabilities for cross customer management at scale for partners to differentiate and benefit from greater efficiency and automation

Automate and scale cloud management

+

Enable greater visibility and governance

+

Grow your market by reaching customers in new ways

Cross tenant management	API extensibility	All licensing supportability	Enhanced visibility

Foundational best practices

The architecture brings greater versatility and a management capabilities into several scenarios

3 Accessing new customer markets, enabling partner to partner scenarios

Marketplace offers (new) | ARM Template | APIs | Managed Apps

2 Cross-tenant experience integrated into Azure and third-party services

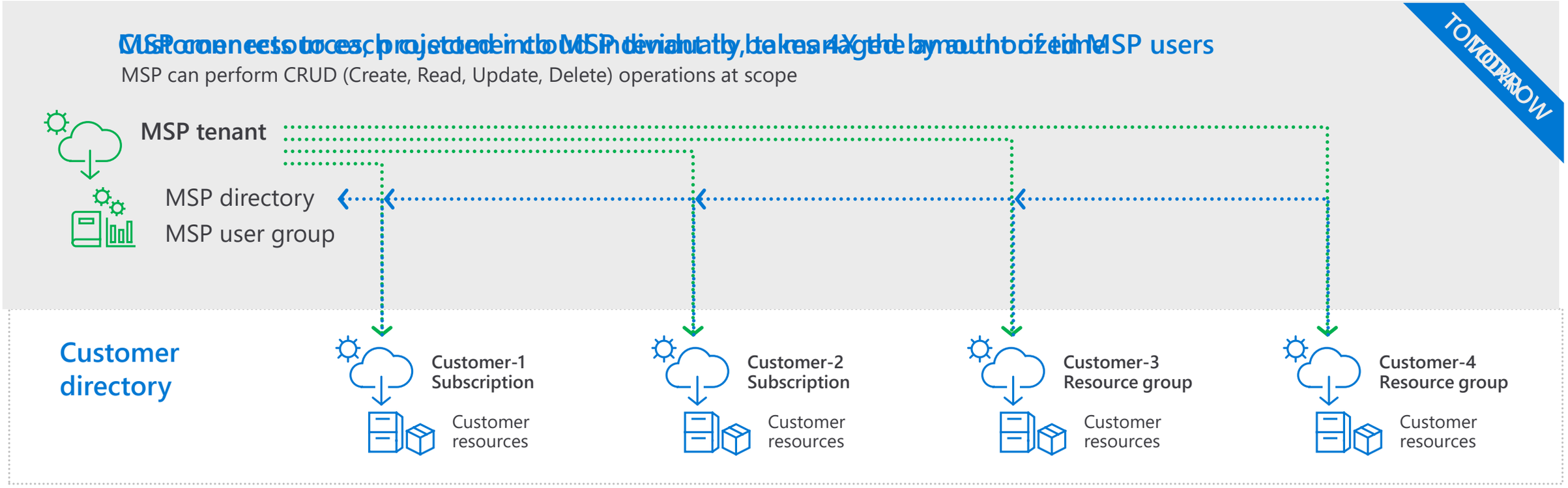
Azure Policy ⊕ Azure Monitor ⊕ Azure Security Center ⊕ Azure Portal ⊕ Azure Kubernetes Service (AKS) ⊕ Azure Virtual Network ⊕ And more...

1 Azure Delegated Resource Management acts as foundational fabric

Azure Resource Manager (ARM) | Azure Identity

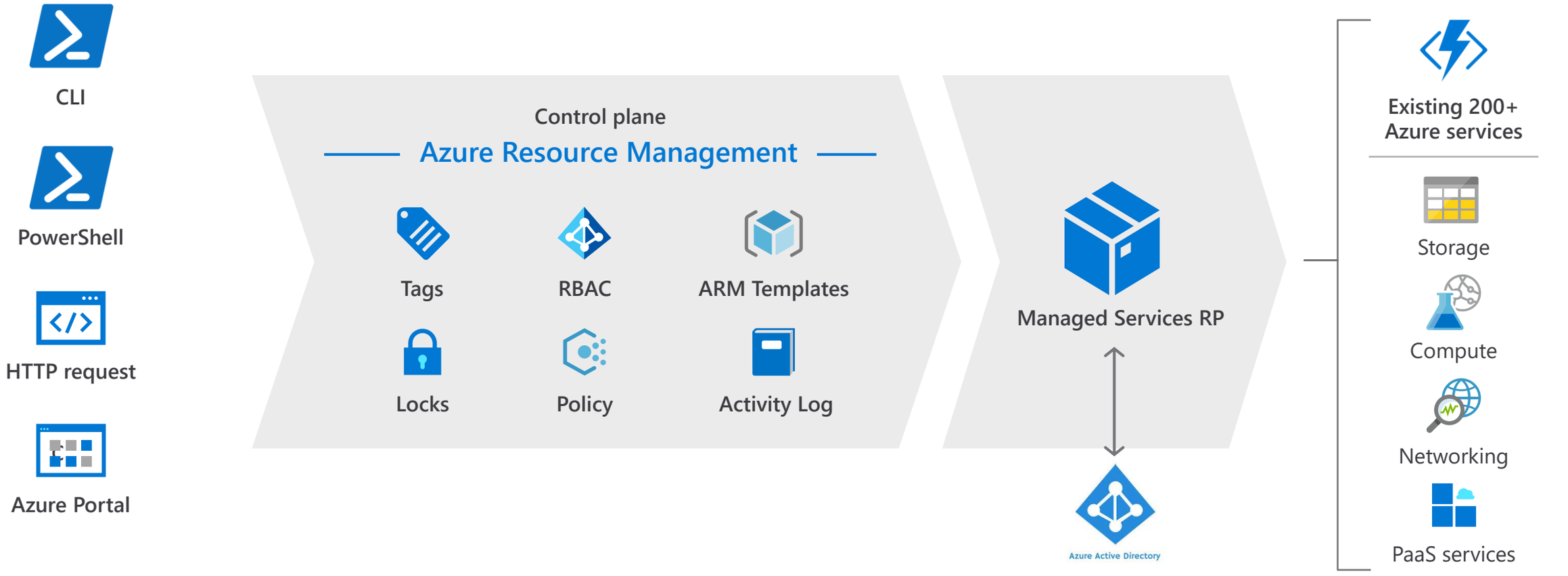
See template and Github repository

The secret sauce to Azure delegated resource management lies in being able to project customer resources into the partners environment



Azure Delegated Resource Management creates logical (control plane) access to customer's environment for the service provider

1. MSP initiates an action for customer resource
2. ARM validates the request is from a partner tenant and calls Managed Service Resource Provider (RP)
3. Managed service RP provides MSPs precise RBAC access
4. MSP completes the action on customer resource



Automate and scale cloud management

Enable greater visibility and governance

Grow your market in new ways

Complex scripting and credential management, creating customer and partner overhead

Today

Azure Managed Service Provider

Managed Service Provider

Script Library

- Automation
- Analytics
- Credential logging

Customer 1

Customer directory

- Deploy VMs
- Set up management alerts
- Manage environment through scripts—update, delete

Customer 2

Customer directory

- Deploy VMs
- Set up management alerts
- Manage environment through scripts—update, delete

Customers have to clean up MSP users manually, they may trade off this manual work for admin access to MSP

Automate and scale cloud management

Enable greater visibility and governance

Grow your market in new ways

Complex scripting and credential management, creating customer and partner overhead

Today

Avanade is managing users in each customer tenant, certificates, expiration dates of user privileges, working with customer for every request.

avanade

Log Analytics directory

- Aggregation
- Analytics
- Insights

If they want more access, Avanade resources have to spend more time explaining complexity of access to customer.

Customer 1

Customer directory

- Deploy VMs
- Set up event Hub as a container of information
- Deploy Azure functions to scrape the data

Customer 2

Customer directory

Customer 3

Customer directory

Azure SQL database | CosmosDB | Azure Key Vault

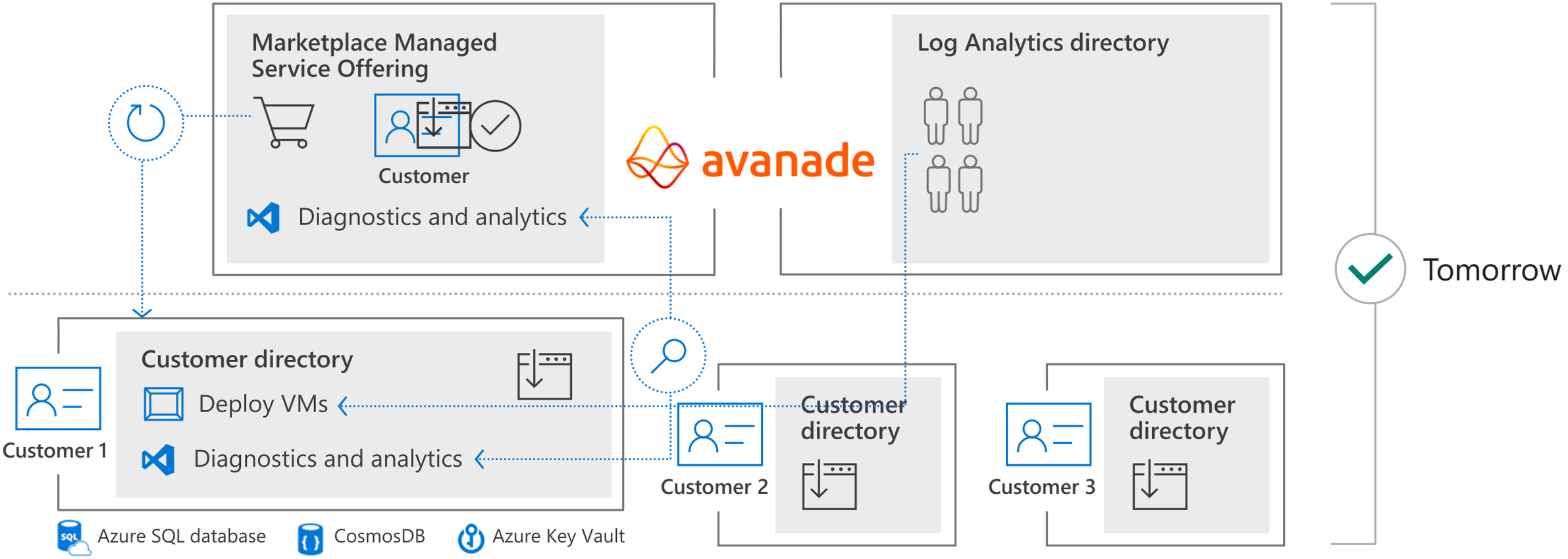
Automate and scale cloud management

Enable greater visibility and governance

Grow your market in new ways

No need to expose your customer to the complexities of setting up the managed service offer. Deploy through marketplace offers that automate managing user groups and enable central partner workspaces to manage all customers.

Data protection to customer | Secured access | Enhanced visibility to customers and partners

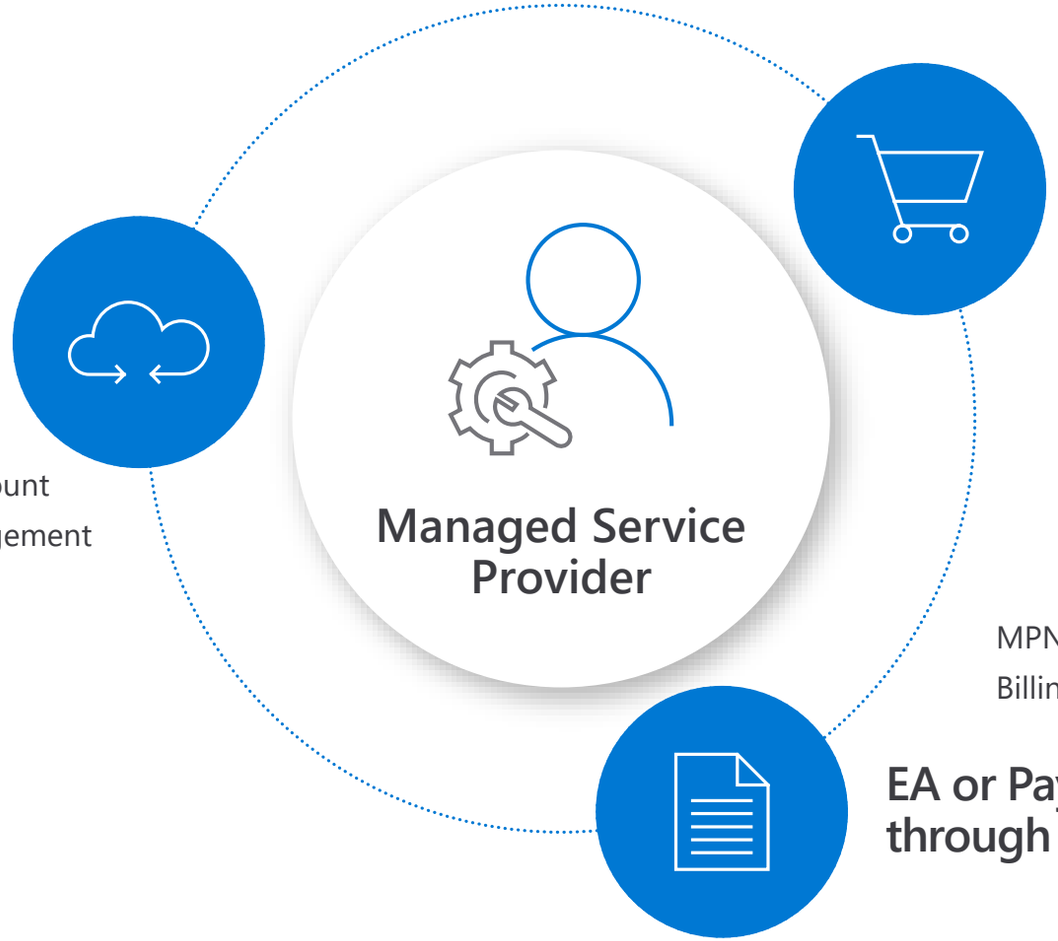


Automate and scale cloud management

Enable your customers with greater visibility and security

Grow your market in new ways

Reduce time to market and onboarding, satisfy compliance requirements and earn partner rewards



Cloud Solution Provider through ARM templates/APIs

Access—full and granular—qualifies for discount

Potential to centralize partner identity management

Billing relationship not impacted

Marketplace

Managed service offers integrated with Azure Lighthouse for automatic access and rewards

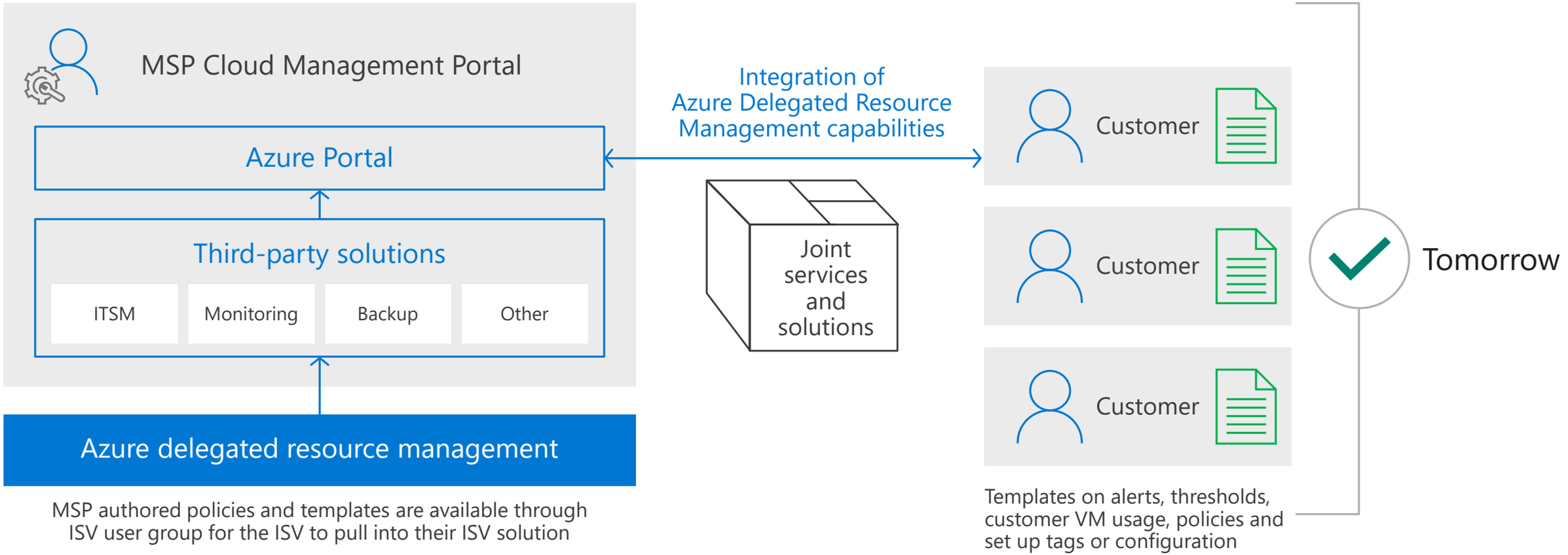
ISV managed apps manifested through Lighthouse to integrate MSP offering into ISV solution

EA or Paygo subscriptions through ARM templates/APIs

MPN id linked through Partner Admin Link (PAL)

Billing relationship unchanged

Automation and cross customer visibility can be demonstrated in ISV solutions being used by Managed Service Providers for customers



Security Operations

Attack services are inexpensive

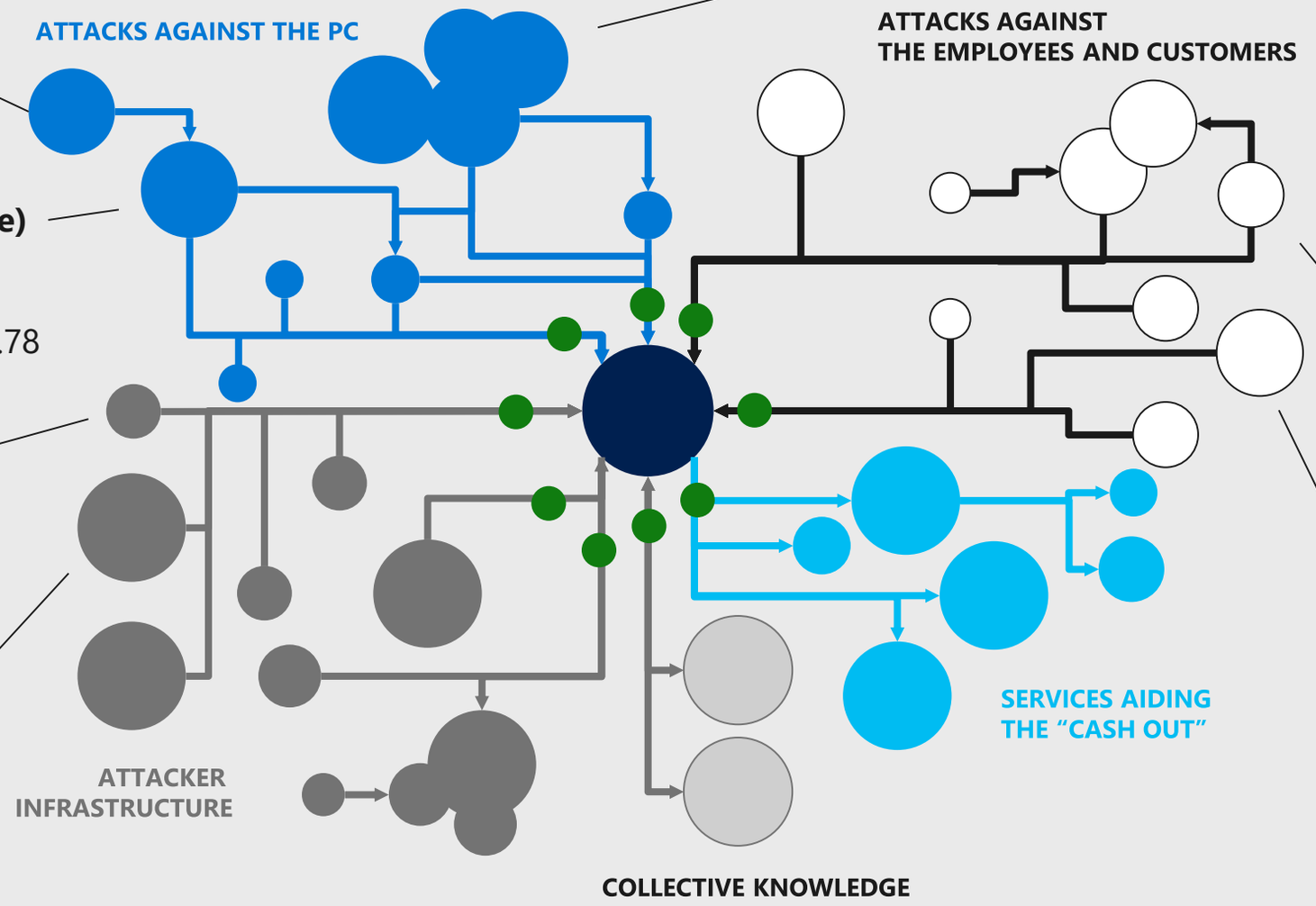
Ransomware:
$66 upfront
Or
30% of the profit (affiliate model)

0days price range varies from $5,000 to $350,000

Loads (compromised device) average price ranges
- **PC** - $0.13 to $0.89
- **Mobile** - from $0.82 to $2.78

Denial of Service (DOS) average prices
day: $102.05
week: $327.00
month: $766.67

Proxy services to evade IP geolocation prices vary
As low as $100 per week for 100,000 proxies.



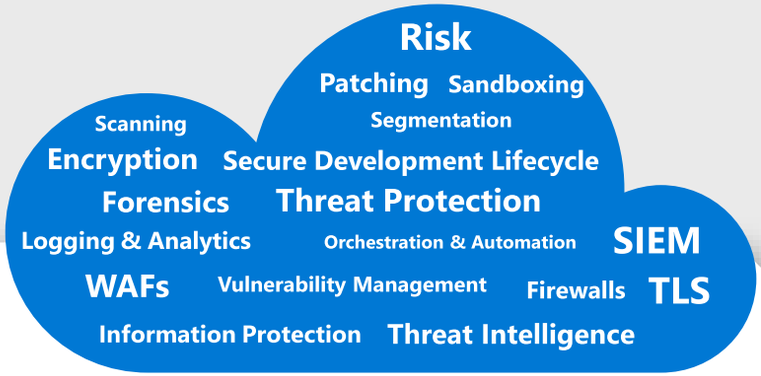
Spearphishing services range from $100 to $1,000 per successful account take over

Compromised accounts
As low as $150 for 400M.
Averages $0.97 per 1k.

Transforming from Legacy to Cloud

Evolving architecture, tools, skills, & practices

MAIN MENU



Architectures change, but principles & outcomes remain the same

Roles, responsibilities, and skillsets will evolve

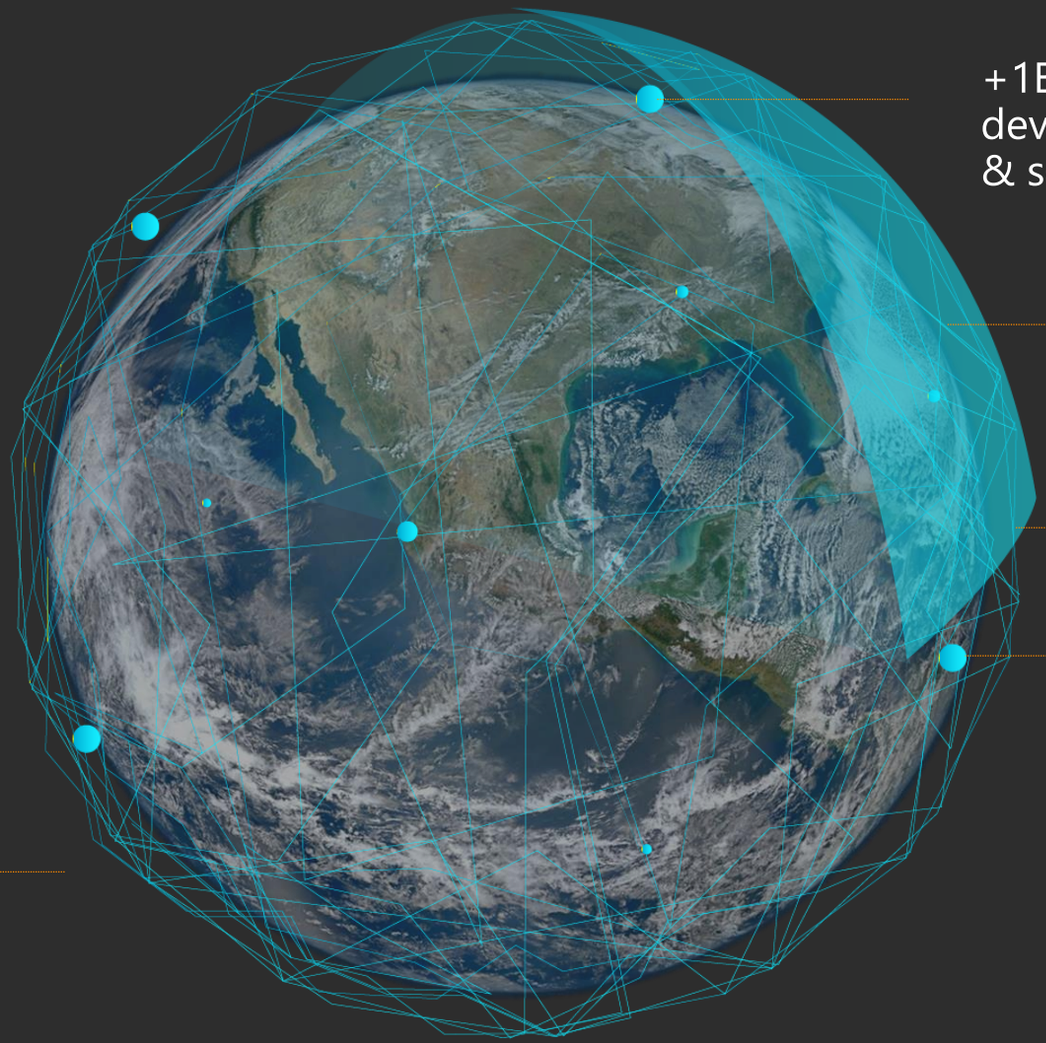
Controls, tools, and processes will evolve

Note: Legacy ‘technical debt’ persists with legacy workloads/applications in IaaS

The Microsoft **Intelligent Security Graph**

Extensive machine learning to:

- Reduce manual effort
- Reduce wasted effort on false positives
- Speed up detection



+1B Windows devices updated & scanned

450B monthly authentications

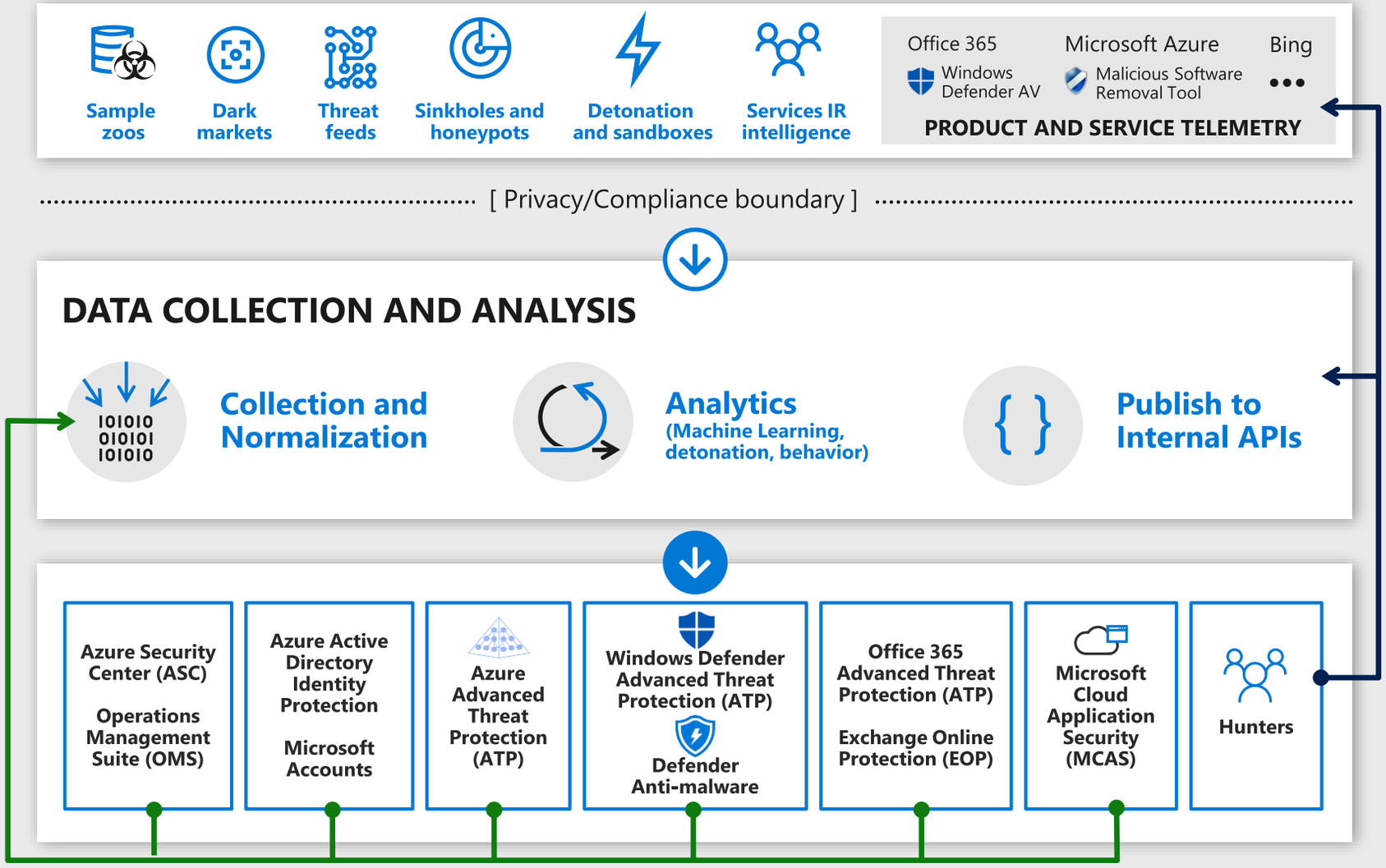
18+ billion web pages scanned

400B e-mails analyzed

930M threats detected on devices every month

Unparalleled cybersecurity visibility and insight

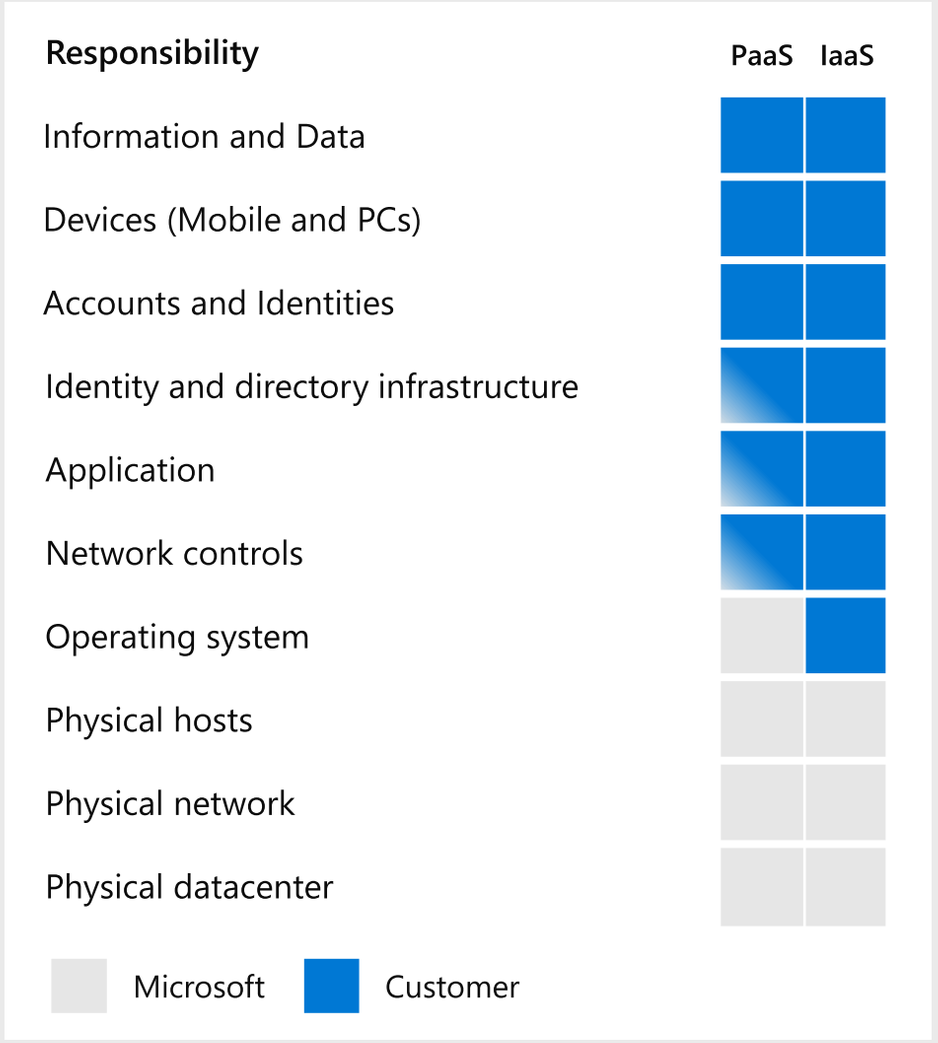
Inside The Intelligent Security Graph



- Products instrumented to strict privacy/compliance standards
  See Microsoft Trust Center
- Analytics help fuel new discoveries
- Products send data to graph
- Products use Interflow APIs to access results
- Products generate data which feeds back into the graph
- Hunters identify attacks, improve analytics, feed back into product design

Security Responsibilities Transfer to Azure

MAIN MENU



Transferred for PaaS

Security Patches

Feature Upgrades

VMs/Containers security –
OS and Middleware Installation, Maintenance, troubleshooting, etc.

Azure Marketplace
fits PaaS or IaaS model

Transferred for IaaS and PaaS

Denial of Service*

Racking/Stacking Servers, Delays in Adding Capacity

Fabric/Virtualization Patching, Maintenance & Troubleshooting

Fabric Availability / Uptime
→ SLA from Microsoft

Attacks on

- Physical Attacks
- Virtualization Fabric
- Hardware/Firmware
- Network Infrastructure

Microsoft protecting Microsoft

Hardening (Physical, OS App/Data, etc.)
Whitelisting
Auto-Patching
and more...

Traditional Defenses

Corporate Infrastructure

Cloud Infrastructure

Continual Scanning
Penetration Testing
Red Team Ops
Bug Bounties
One Hunt

Attackers View

People

Background Checks
Security Training
Conferences

Least Privilege

Least Privilege Access
Just-in-time Access
and more...

Authentication

Multi-factor Auth
Anomaly Detection

Privileged Access Workstations

Secure Access Workstations
isolation from web/email risks

Rigorous Security For Privileged Access

Automated Assessments
Secure DevOps toolkit
and more...

Security Development Lifecycle

Continuous Logging & Monitoring
Incident Response
CDOC (24x7 SOC)

Monitoring & Vigilance

Red Team

VS

Blue Team

ONEHUNT

Cybersecurity Reference Architecture

May 2018 – https://aka.ms/MCRA | Video Recording | Strategies

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Security Operations Center (SOC)

- Vulnerability Management
- MSSP
- SIEM + Analytics
- Cybersecurity Operations Service (COS)
- Incident Response and Recovery Services
- Azure Security Center
- Windows Defender
- Office 365 Security & Compliance
- Azure
- Cloud App Security
- Advanced Threat Protection (ATP)
- Graph Security API *(Public Preview)*
- Alert & Log Integration

Software as a Service

Office 365
- Secure Score
- Customer Lockbox

Dynamics 365

Identity & Access

- Azure Active Directory
- Conditional Access – Identity Perimeter Management
- Azure AD Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
- Azure AD PIM
- Multi-Factor Authentication
- Azure AD B2B
- Azure AD B2C
- Hello for Business
- MIM PAM
- Azure ATP
- Active Directory
- ESAE Admin Forest

Information Protection

- Cloud App Security
- Azure Information Protection (AIP)
  - Discover
  - Classify
  - Protect
  - Monitor
  - *Hold Your Own Key (HYOK)*
  - AIP Scanner
- Classification Labels
- Office 365
  - Data Loss Protection
  - Data Governance
  - eDiscovery
- Azure SQL Threat Detection
- SQL Encryption & Data Masking
- Azure SQL Info Protection *(Preview)*
- Endpoint DLP

Clients

Unmanaged & Mobile Devices

- Intune MDM/MAM

Managed Clients

- System Center Configuration Manager
- Windows Defender ATP
  - Secure Score
  - Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s) | 3rd party IaaS | Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

- Configuration Hygiene
- Just in Time VM Access
- Adaptive App Control

Extranet
- NGFW
- Edge DLP
- SSL Proxy
- IPS

Security Appliances

Express Route

Intranet Servers
- Windows Server 2016 Security
  Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...
- Shielded VMs
- Azure Stack
- VMs

Privileged Access Workstations (PAWs)

- Azure Policy
- Azure Key Vault
- Azure WAF
- Azure Antimalware
- Application & Network Security Groups
- Backup & Site Recovery
- Disk & Storage Encryption
- Confidential Computing
- DDoS attack Mitigation+Monitor

Windows 10 Enterprise Security

- Network protection
- Credential protection
- Exploit protection
- Reputation analysis
- Full Disk Encryption
- Attack surface reduction
- App control
- Isolation
- Antivirus
- Behavior monitoring

S Mode

IoT and Operational Technology

- Windows 10 IoT
- Azure IoT Security
- Azure Sphere
- IoT Security Maturity Model
- IoT Security Architecture

Included with Azure (VMs/etc.) Premium Security Feature

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center | Intelligent Security Graph

Microsoft

Identity and Access Management

Identity

CRITICAL BEST PRACTICES

BLOCK LEGACY AUTHENTICATION

- **What –** Block legacy authentication protocols for Azure AD
- **Why** – Weaknesses in older protocols are actively exploited by attackers every day, particularly for password spray attacks (majority use legacy auth)
- **How** – Configure Conditional Access to block legacy protocols

https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Conditional-Access-support-for-blocking-legacy-auth-is/ba-p/245417

For more information
https://www.youtube.com/watch?v=wGk0J4z90GI

DON'T SYNCH AD ADMINS

- **What –** Don't synchronize accounts to Azure AD that have high privileges in your existing Active Directory
- **Why –** This mitigates the risk of adversaries pivoting from cloud to on premises assets (creating a potential major incident).
- **How –** This is blocked by default. Do not change the default Azure AD Connect configuration that filters out these accounts

See also the converse guidance in Administration section:

- ***Critical Impact Admin - Account***
- ***Critical Impact Admin - Workstation***

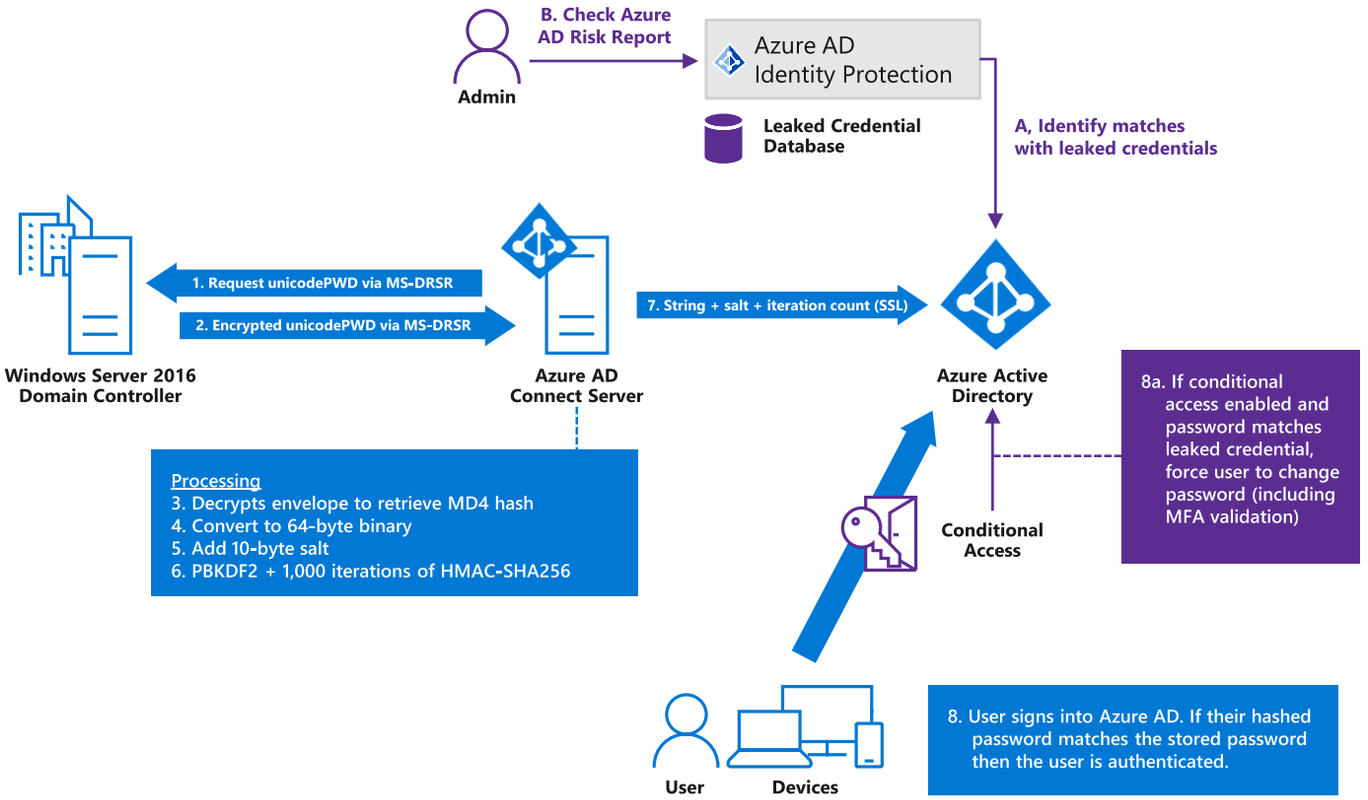
Identity – Password Synchronization

CRITICAL BEST PRACTICE

SYNCHRONIZE PASSWORD HASHES

- **What** – Synchronize your user password hashes from on-premises Active Directory instance to Azure Active Directory (Azure AD).
- **Why –** This increases both
  - **Security** - Protect against leaked credentials being replayed from previous attacks
  - **Reliability** - Customers affected by (Not)Petya attacks were able to continue business operations when password hashes were synced to Azure AD (vs. near zero IT functionality when not)
- **How –** Configure Azure AD Connect to synchronize password hashes

  https://docs.microsoft.com/azure/active-directory/connect/active-directory-aadconnectsync-implement-password-hash-synchronization



Identity –Password Protection from Cloud

CRITICAL BEST PRACTICES

AZURE AD PASSWORD PROTECTION

- **What –** Choose the level of password protection in Azure Active Directory
- **Why** – Static on-premises defenses capabilities can no longer protect password-based accounts.
  - **Microsoft -** https://www.microsoft.com/en-us/research/publication/password-guidance/
  - **NIST** - https://pages.nist.gov/800-63-3/sp800-63b.html

Passwordless solutions are ideal and MFA can help, but passwords should also be strengthened

How – Choose protection for Azure AD Passwords

2. Automatic Enforcement

Automatically remediate high risk passwords with Conditional Access (leveraging Azure AD Identity Protection risk assessments)

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview

1. Report & Remediate

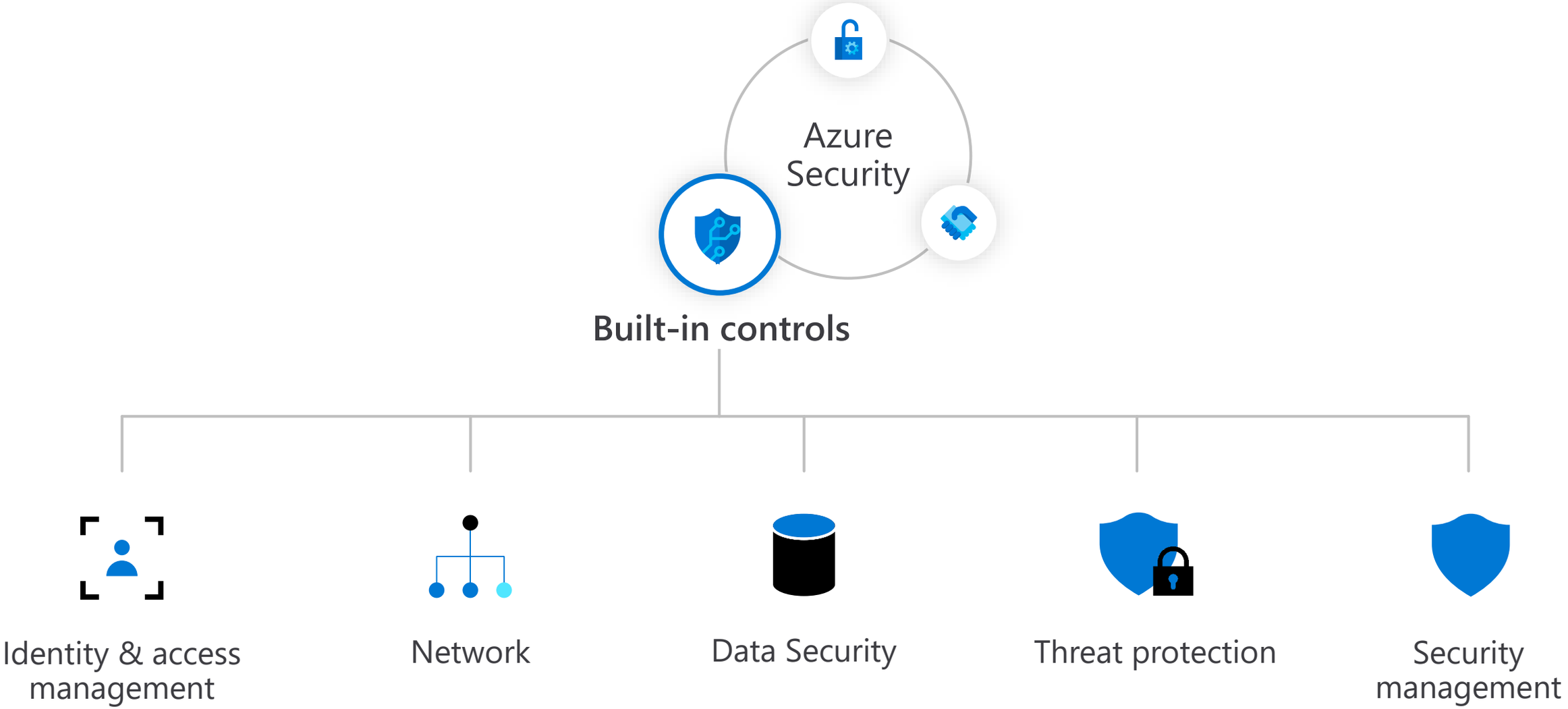
View reports and manually remediate accounts

- **Azure AD reporting** - Risk events are part of Azure AD's security reports. For more information, see the users at risk security report and the risky sign-ins security report.
- **Azure AD Identity Protection** - Risk events are also part of the reporting capabilities of Azure Active Directory Identity Protection.
- Use the Identity Protection risk events API to gain programmatic access to security detections using Microsoft Graph.

~~0. Do Nothing (Not Recommended)~~

Azure Security Center

Azure Security Center



Azure Security Center

Strengthen security posture

Cloud security posture management

Secure Score

Policies and compliance

Protect against threats

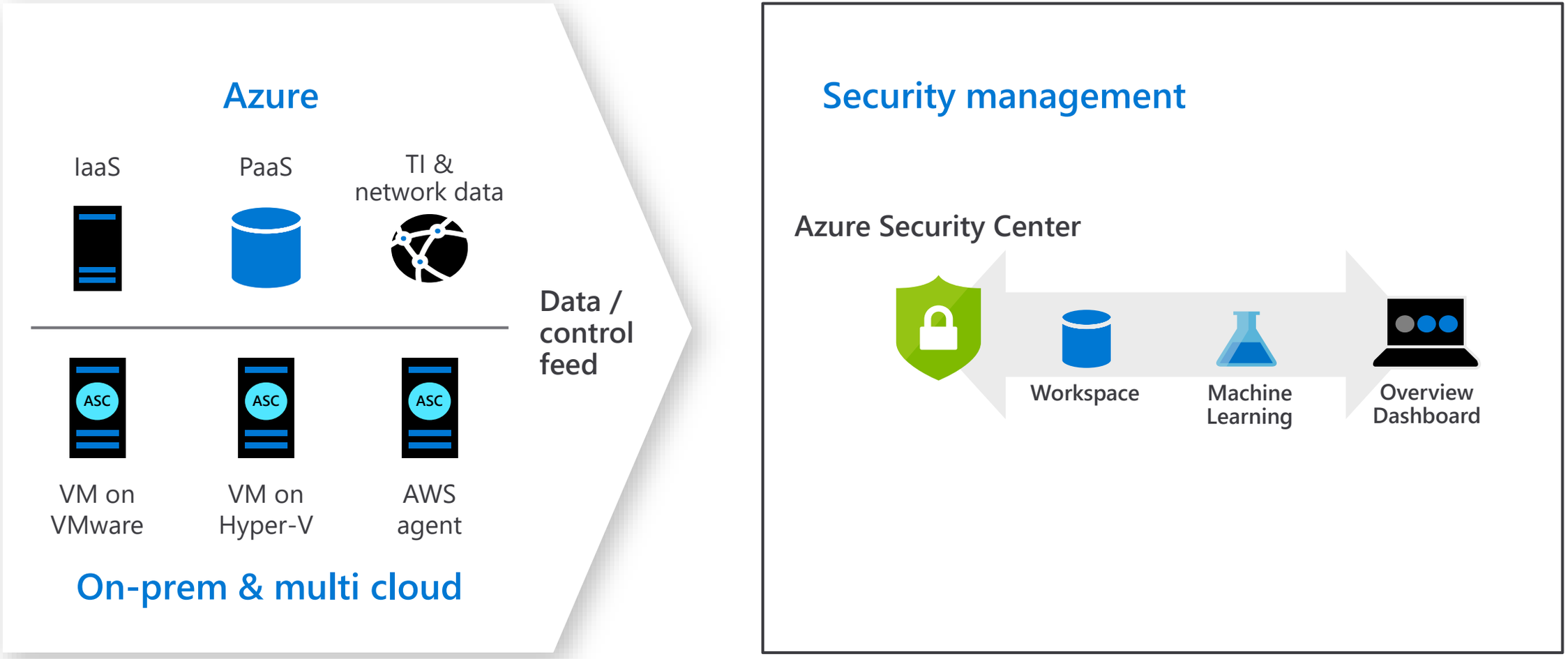
For servers

For cloud native workloads

For databases and storage

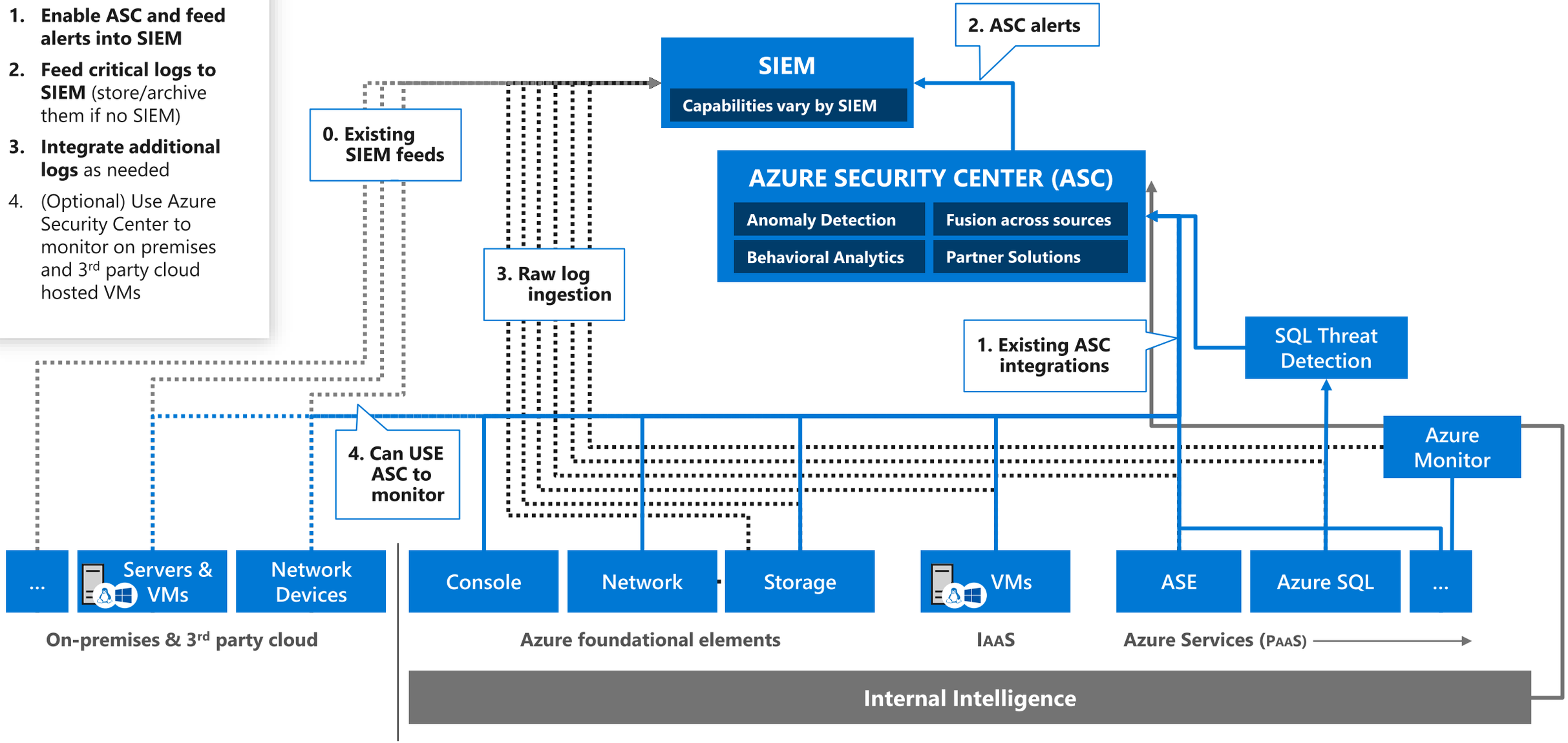
Get secure faster

Azure Security Center Architecture



Getting Visibility in Azure

1. **Enable ASC and feed alerts into SIEM**
2. **Feed critical logs to SIEM** (store/archive them if no SIEM)
3. **Integrate additional logs** as needed
4. (Optional) Use Azure Security Center to monitor on premises and 3rd party cloud hosted VMs

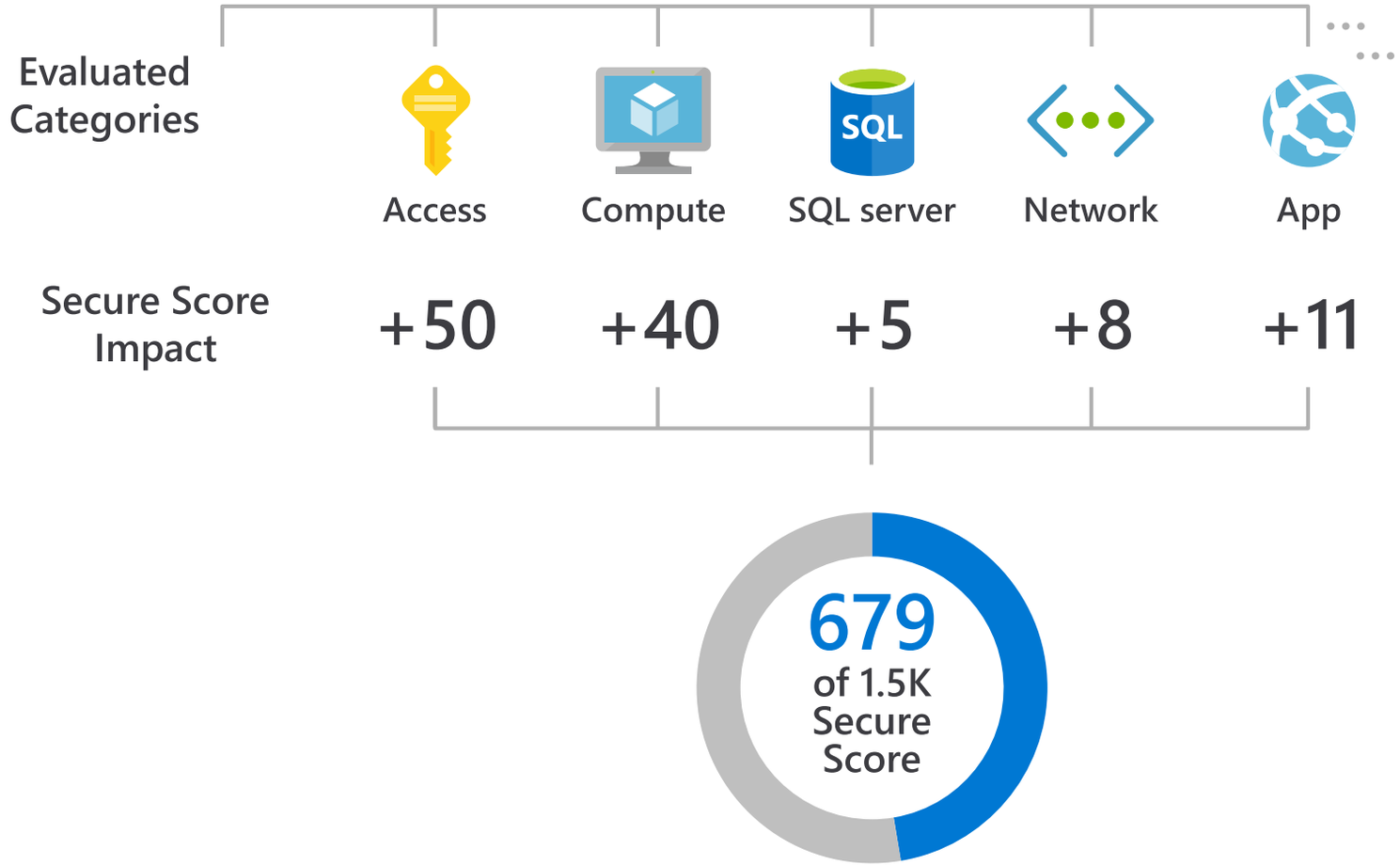


Prioritize your response to security issues with Secure Score

Gain instant insight into the security state of your cloud workloads

Address security vulnerabilities with prioritized recommendations

Improve your Secure Score and overall security posture in minutes

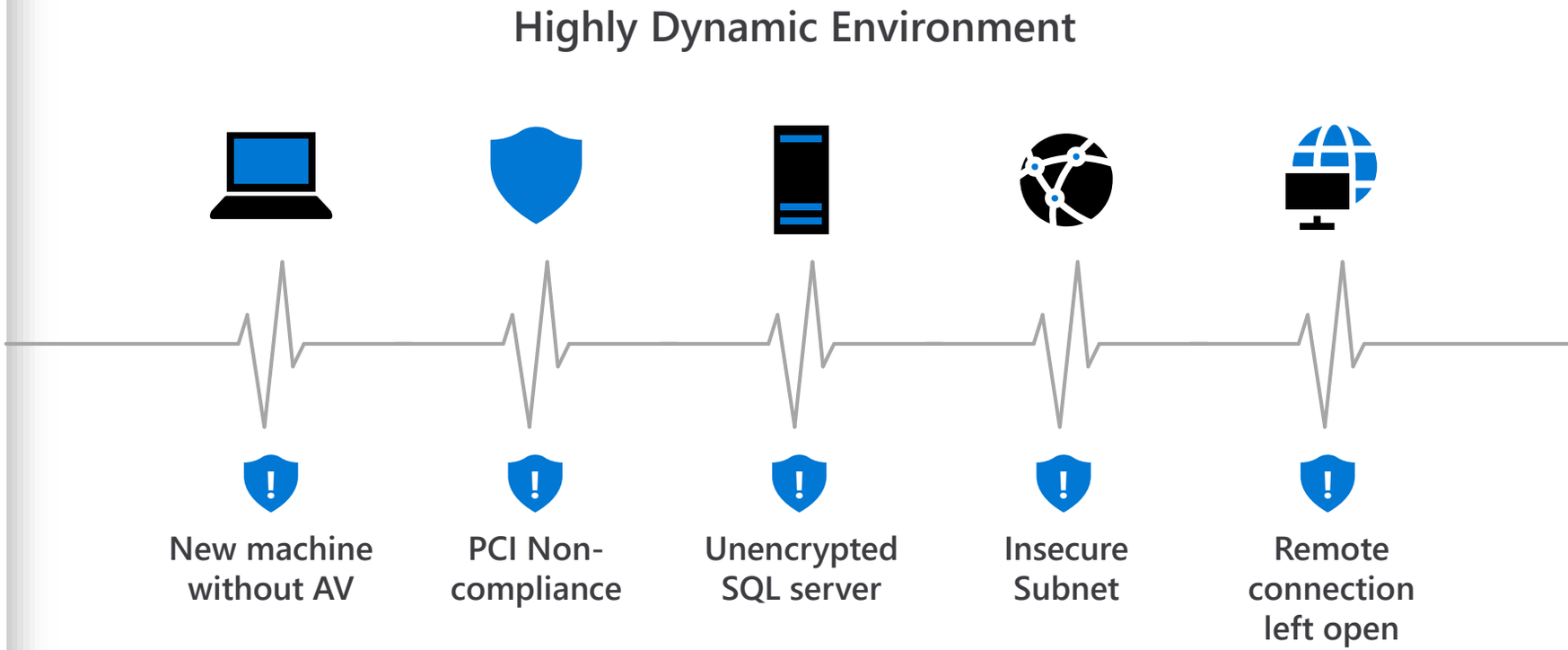


Manage organizational security policies and assess compliance in minutes

Manage security policies at an organizational level

Easily set security policies for subscriptions or management groups

Instantly understand your current policy compliance and review compliance overtime



Azure Security Center

Strengthen security posture

Cloud security posture management

Secure Score

Policies and compliance

Protect against threats

For servers

For cloud native workloads

For databases and storage

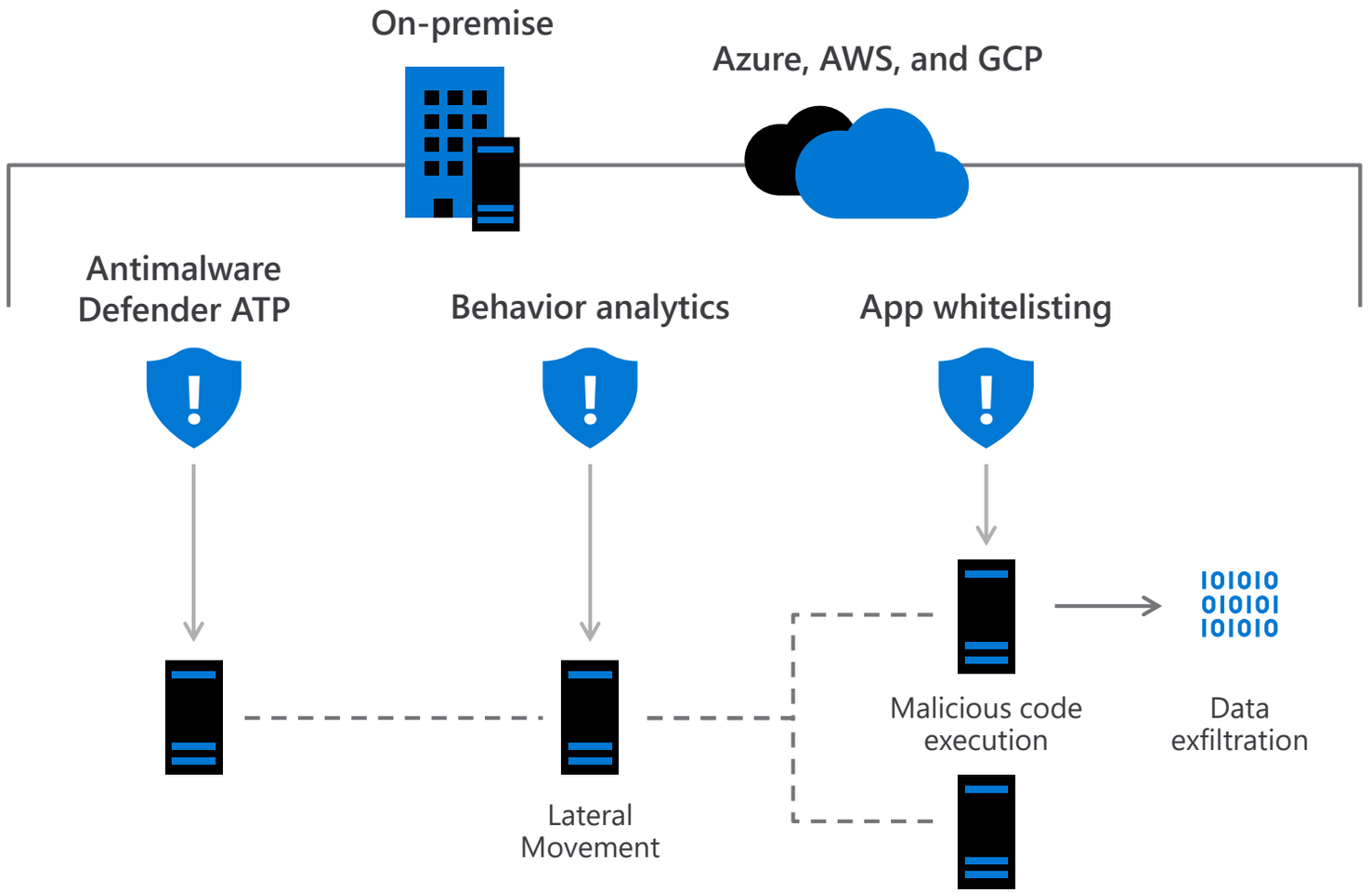
Get secure faster

Protect Linux and Windows servers from threats

Use Just-in-Time VM to control access to commonly attacked management ports

Enable controls to block malicious applications, especially those missed by antimalware solutions, from running

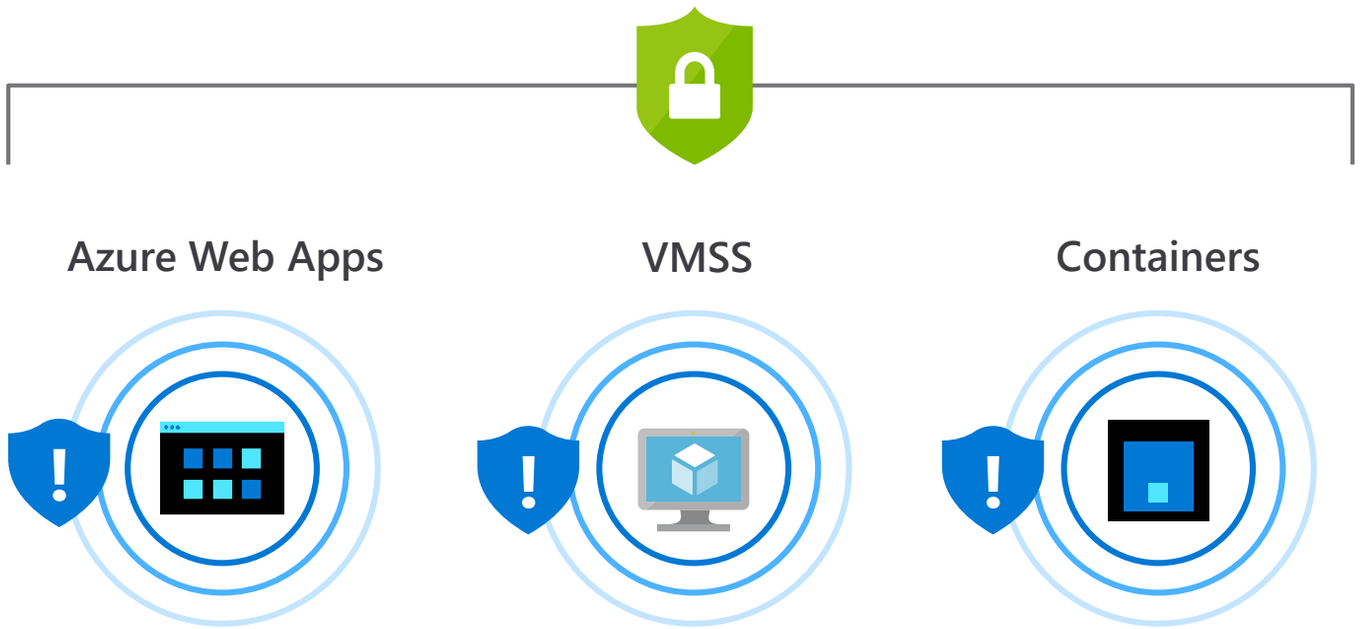
Protect Windows servers and clients with the integration of Windows Defender ATP and Linux servers



Protect cloud-native services from threats

Detect and alert on abnormal admin behavior or compromised web applications

Protects VMSS and containers from malicious attacks

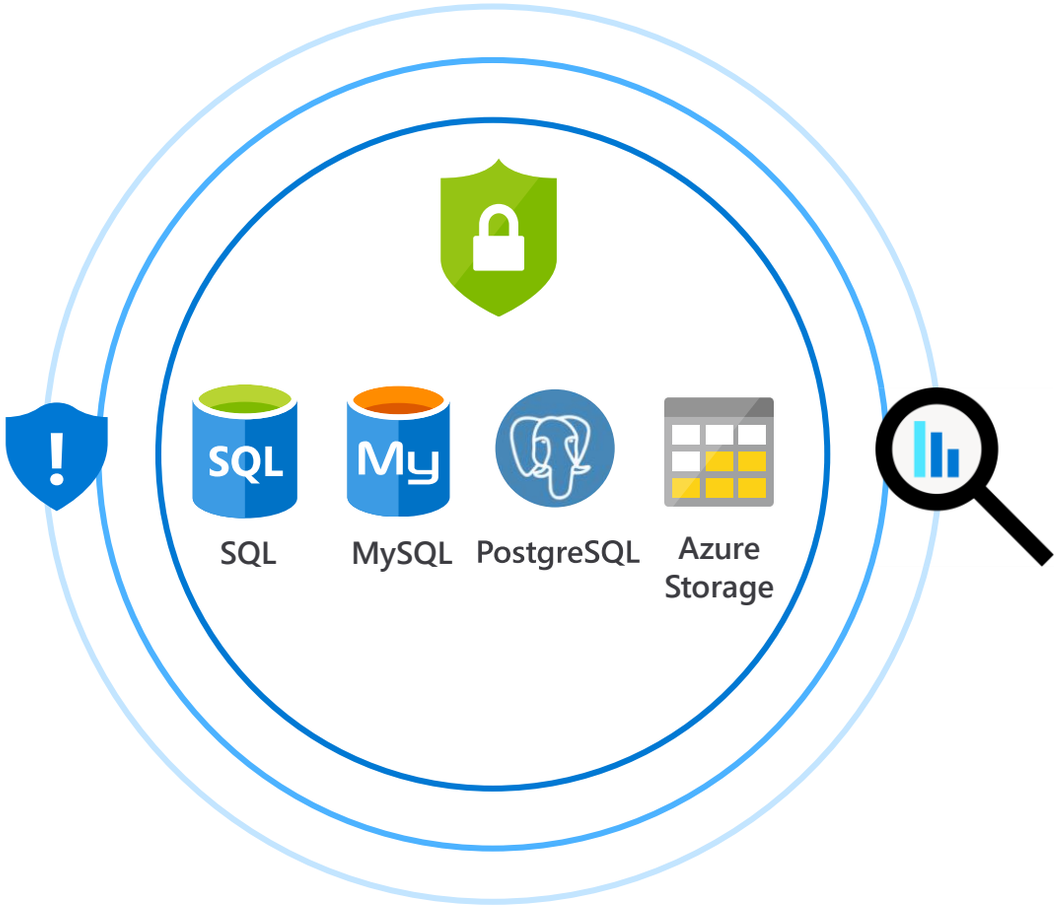


Protect data services from threats

Detect attacks targeting your SQL databases, My SQL, PostgreSQL, and storage accounts

Mitigate threats targeting your Azure SQL databases and configure security best practices

Discover, classify, label and protect sensitive data in your databases



Azure Security Center

Strengthen security posture

Cloud security posture management

Secure Score

Policies and compliance

Protect against threats

For servers

For cloud native workloads

For databases and storage

Get secure faster

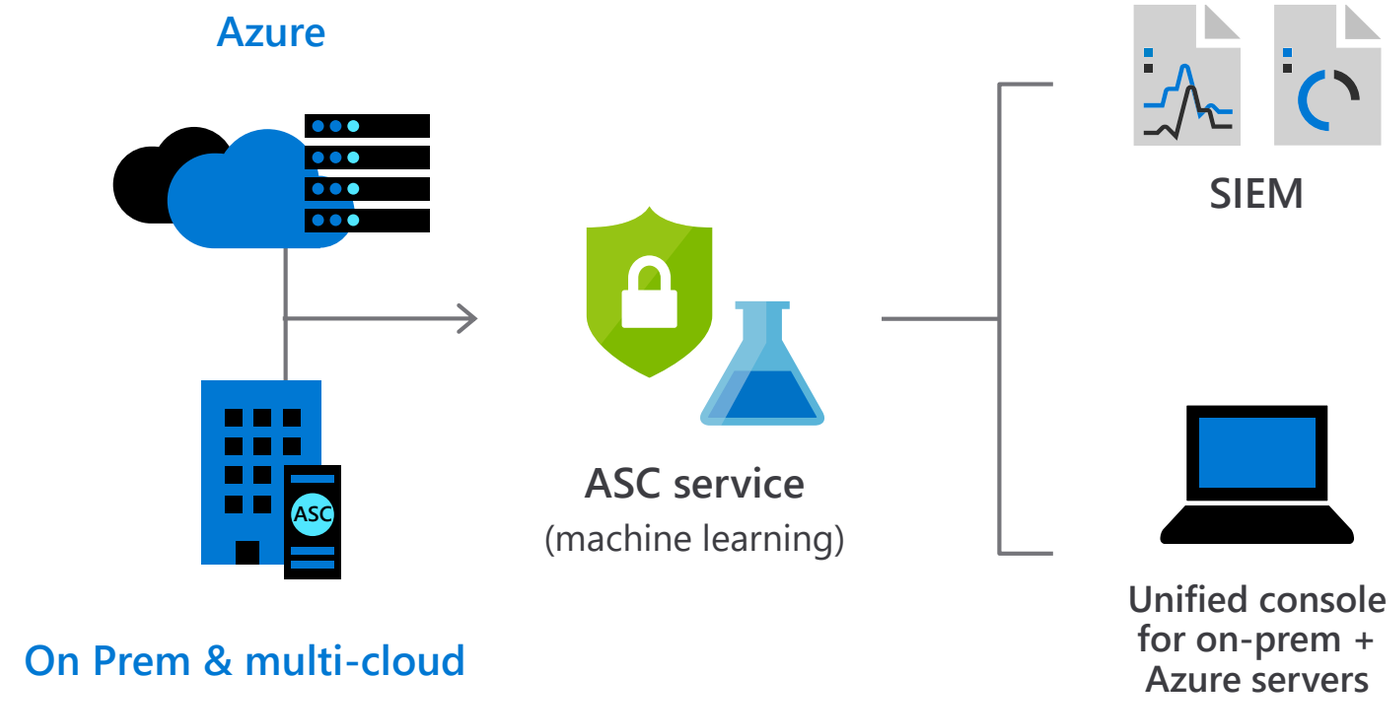
Get secure faster

Automatically discover and onboard Azure resources

Gain a unified view of security across your hybrid cloud workloads

Integrate with existing SIEM or partner solutions to streamline threat mitigation

Assess compliance in a click



Pricing

Features	**Free** (Azure resources only)	**Standard** (Hybrid incl. Azure)
Security policy, assessment, and recommendations	✓	✓
Connected partner solutions	✓	✓
Just-in-time VM Access	--	✓
Adaptive application controls	--	✓
File integrity monitoring	--	✓
Advanced threat detection for networks, VMs/servers, and Azure services	--	✓
Threat intelligence	--	✓
Virtual machines		✓
App Services		✓
SQL databases		✓
Price	Free	$15 / node / month

Azure Sentinel

Traditional SOC Challenges

Sophistication of threats

High volume of noisy alerts

IT deployment & maintenance

Rising infrastructure costs and upfront investment

Too many disconnected products

Lack of automation

Security skills in short supply

Security
Operations Team

Cloud + Artificial Intelligence

Introducing Microsoft Azure Sentinel

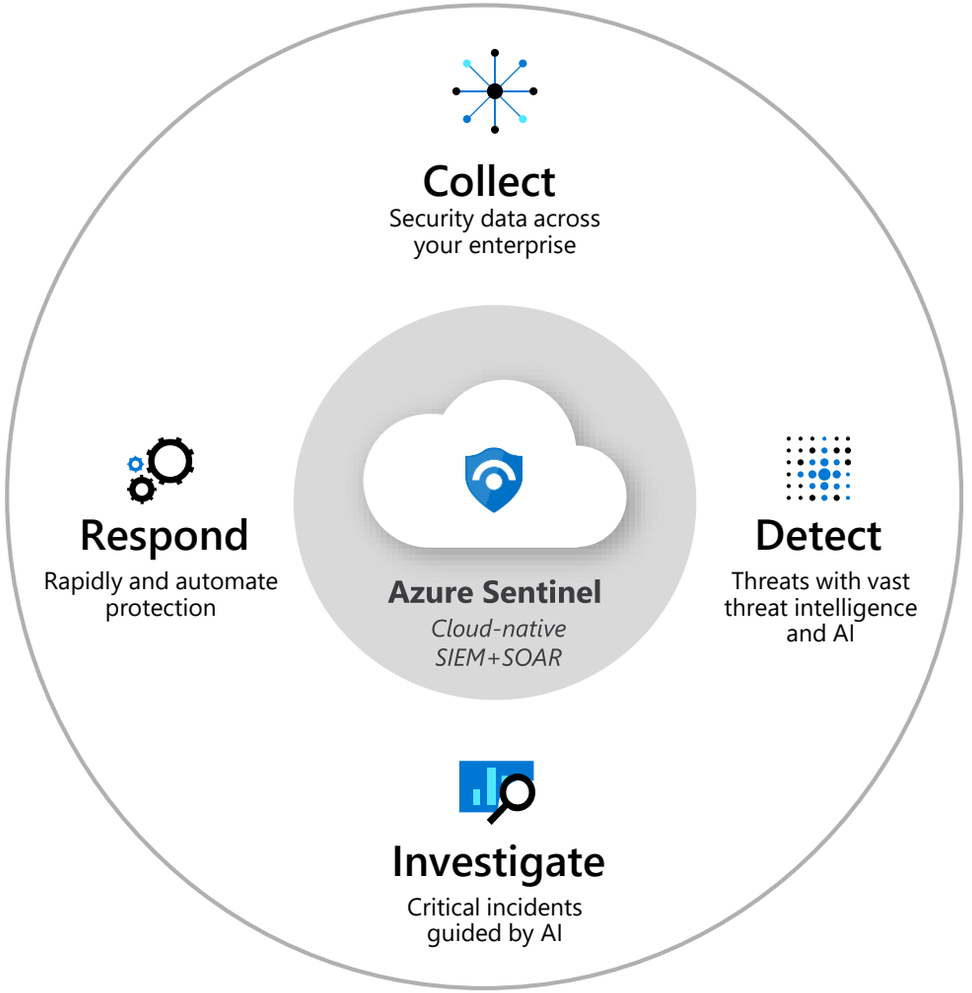
Cloud-native SIEM for intelligent security analytics for your entire enterprise

Limitless cloud speed and scale

Bring your **Office 365 data for Free**

Easy integration with your **existing tools**

Faster threat protection with **AI by your side**

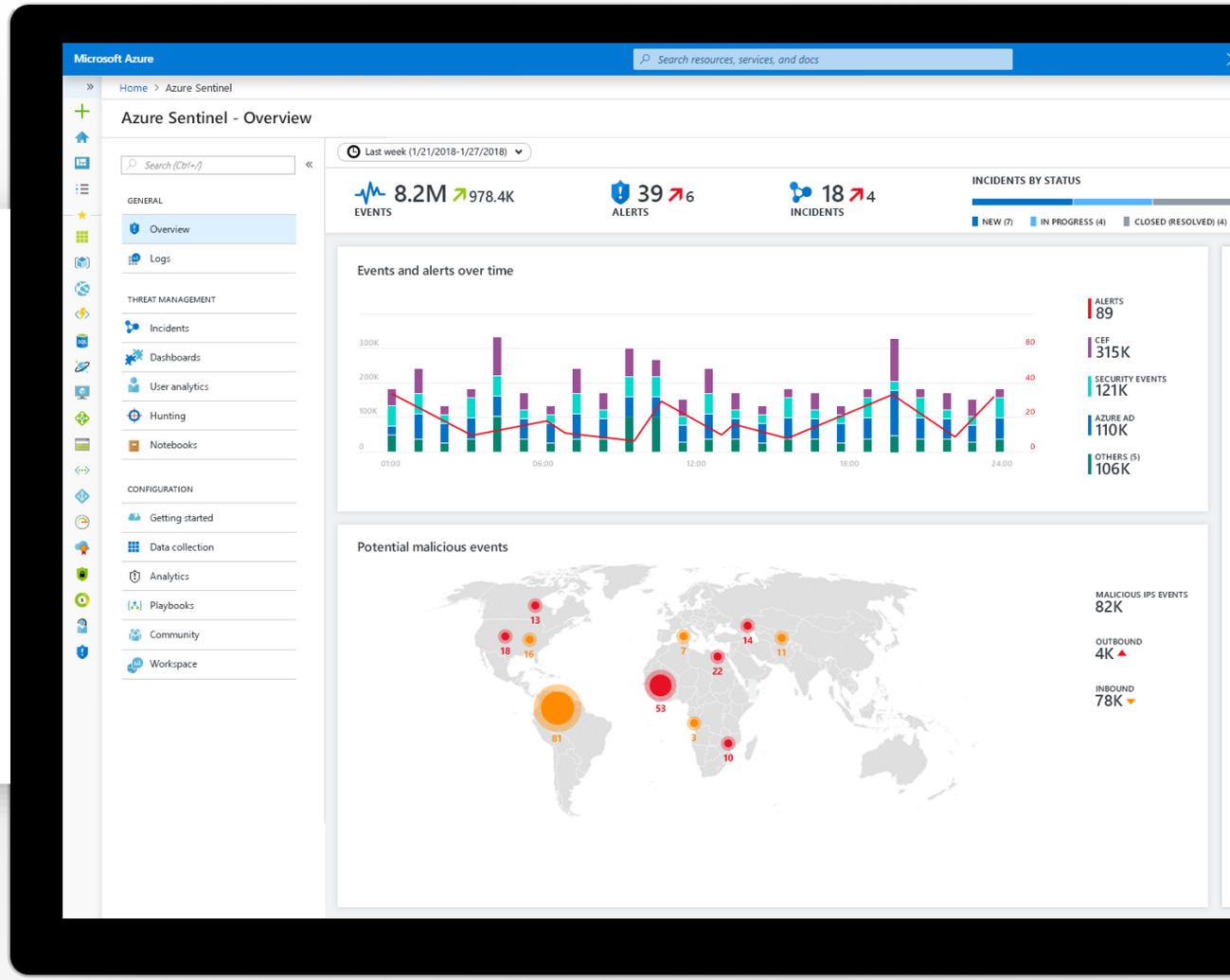


Focus on security, unburden SecOps from IT tasks

No infrastructure setup or maintenance

SIEM Service available in **Azure portal**

Scale automatically, put no limits
to compute or storage resources



Reduce security and IT costs

No infrastructure costs or upfront commitment

Only pay for what you use

Bring your Office 365 Data for free

Cloud-native, scalable SIEM

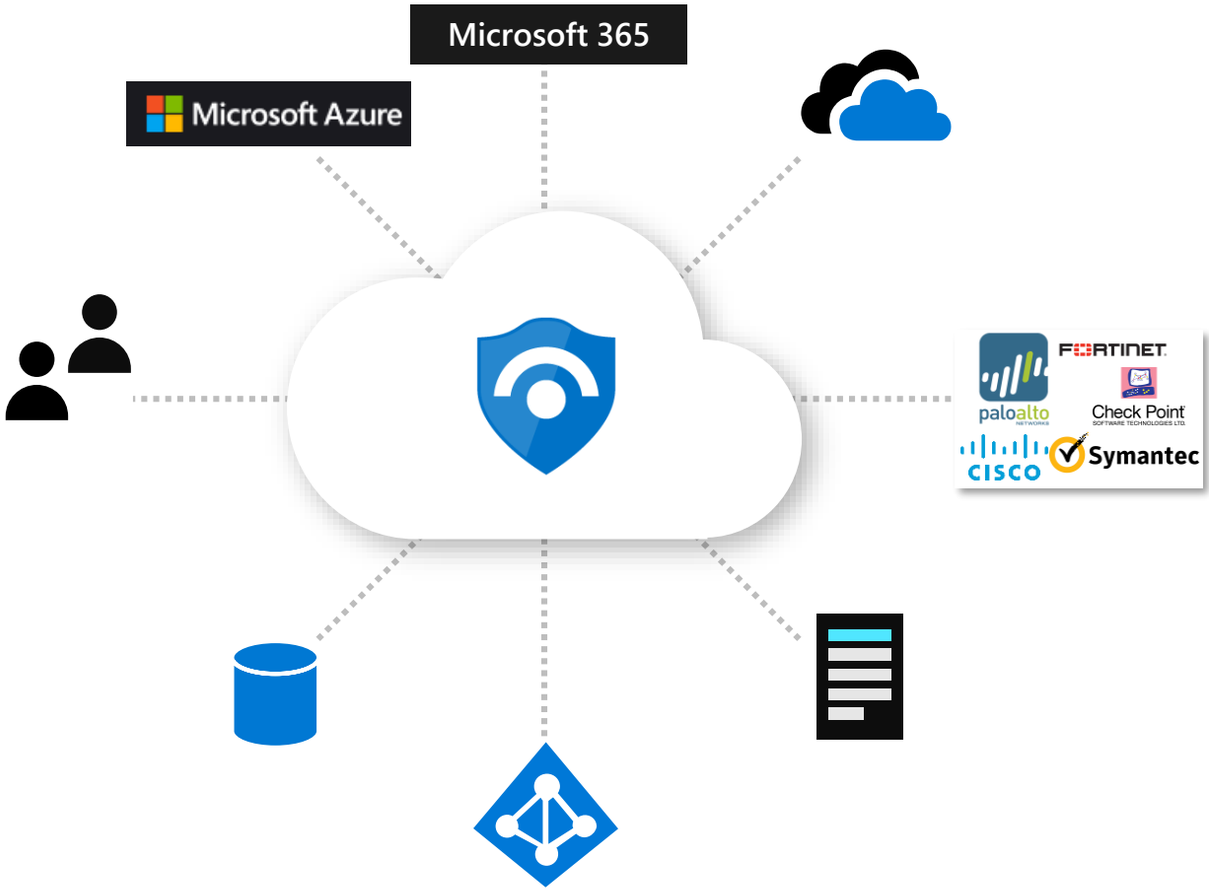
Collect security data at cloud scale from all sources across your enterprise

Pre-wired integration with Microsoft solutions

Connectors for many partner solutions

Standard log format support for all sources

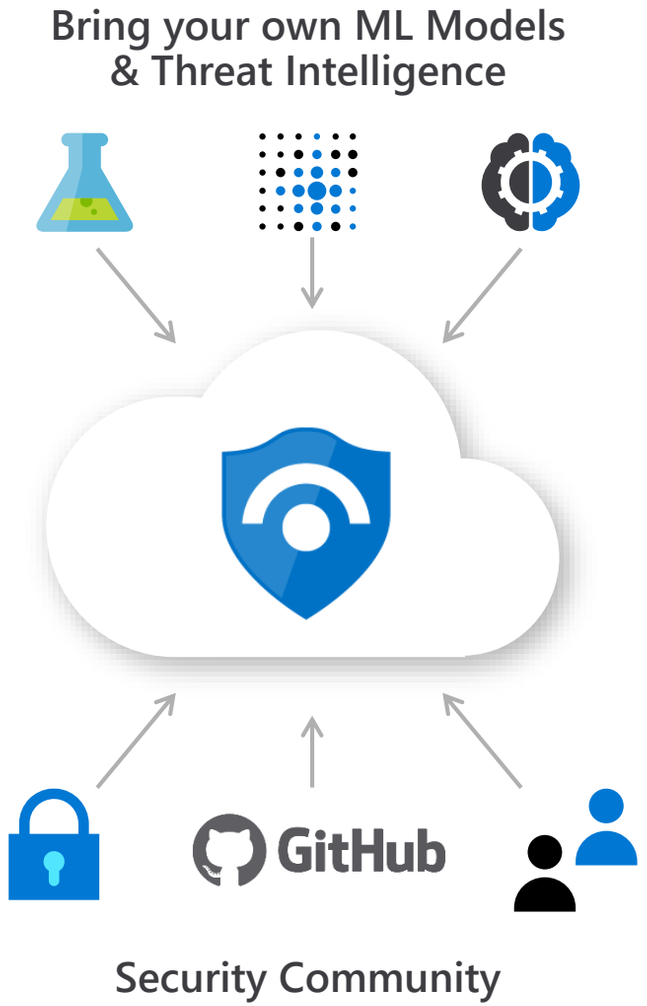
Proven log platform with **more than 10 petabytes** of daily ingestion



Optimize for your needs

Bring your own insights, machine learning models, and threat intelligence

Tap into our **security community** to build on detections, threat intelligence, and response automation.



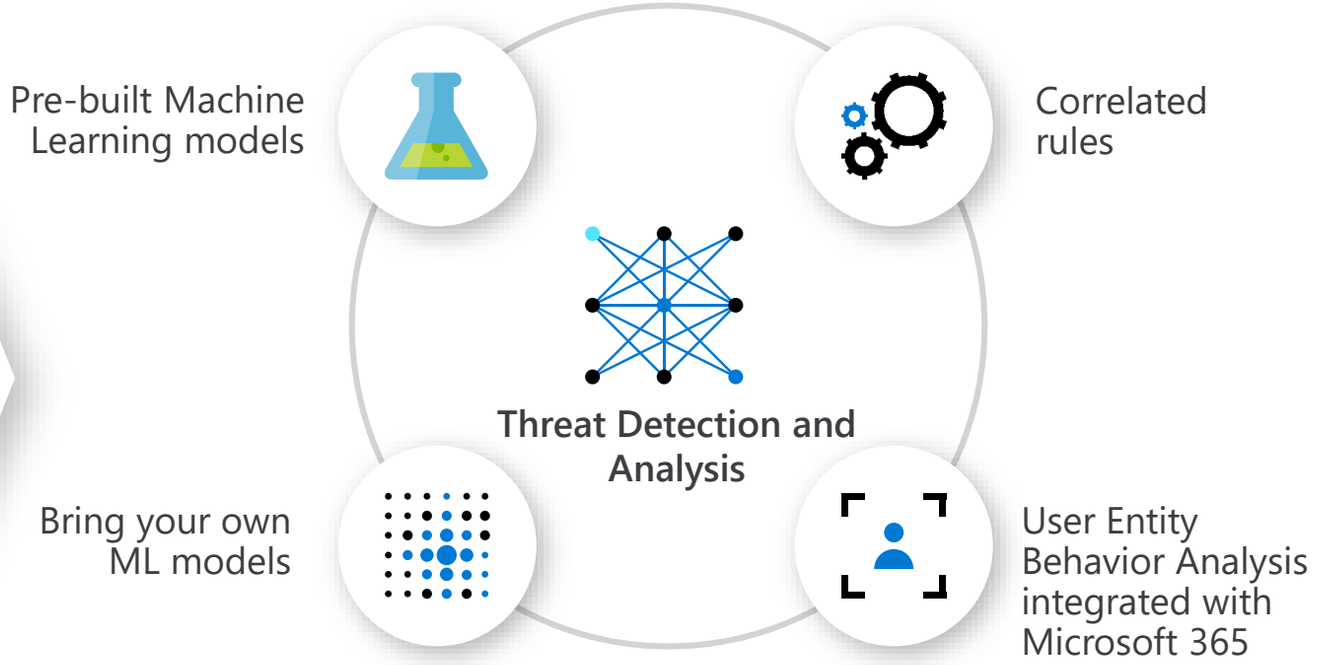
Detect threats and analyze security data quickly with AI

ML models based on **decades of Microsoft security experience and learnings**

Millions of signals filtered to few **correlated and prioritized incidents**

Insights based on vast **Microsoft threat intelligence** and your own TI

Reduce alert fatigue by up to 90%

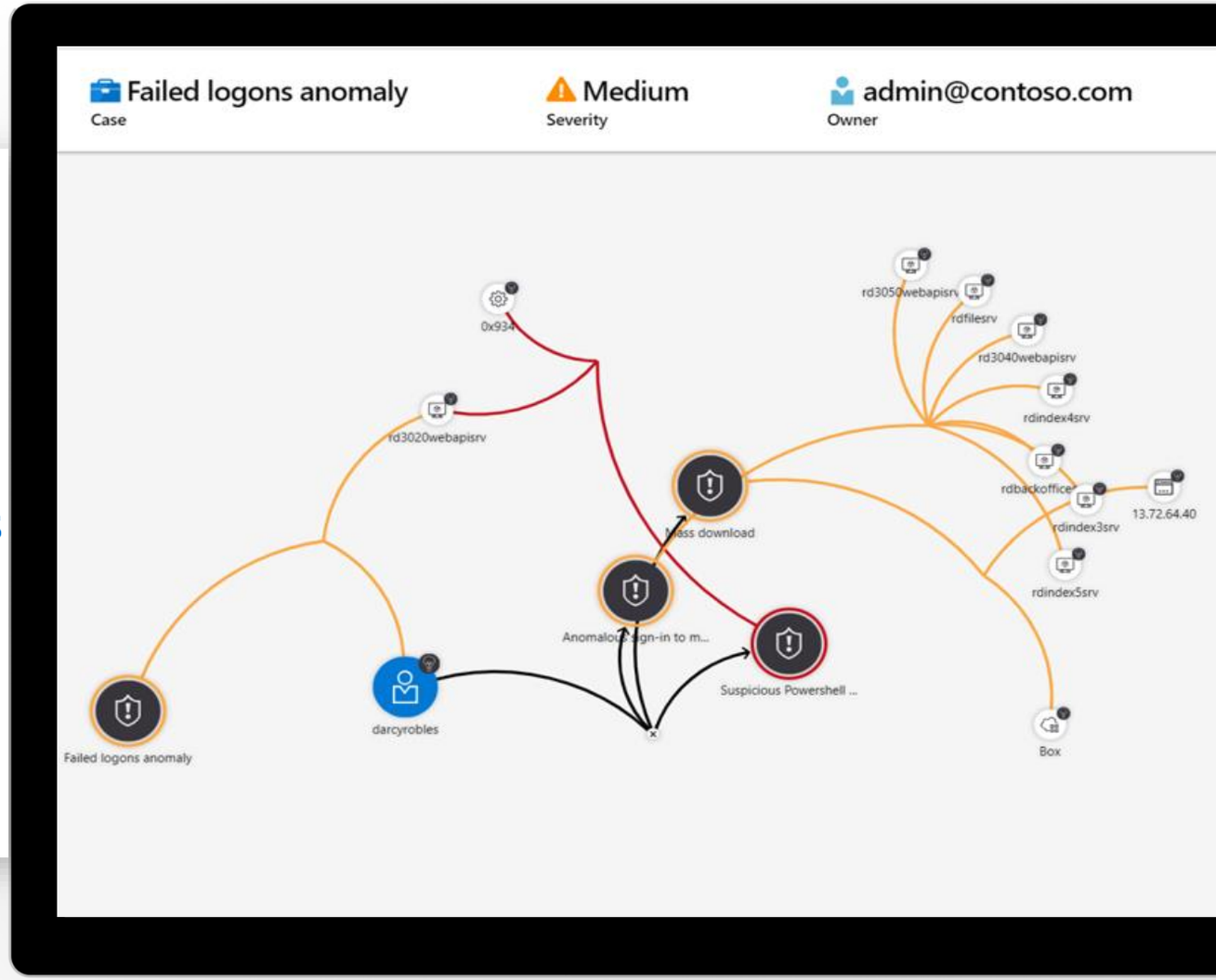


Investigate threats with AI and hunt suspicious activities at scale, tapping into years of cybersecurity work at Microsoft

Get prioritized alerts and **automated expert guidance**

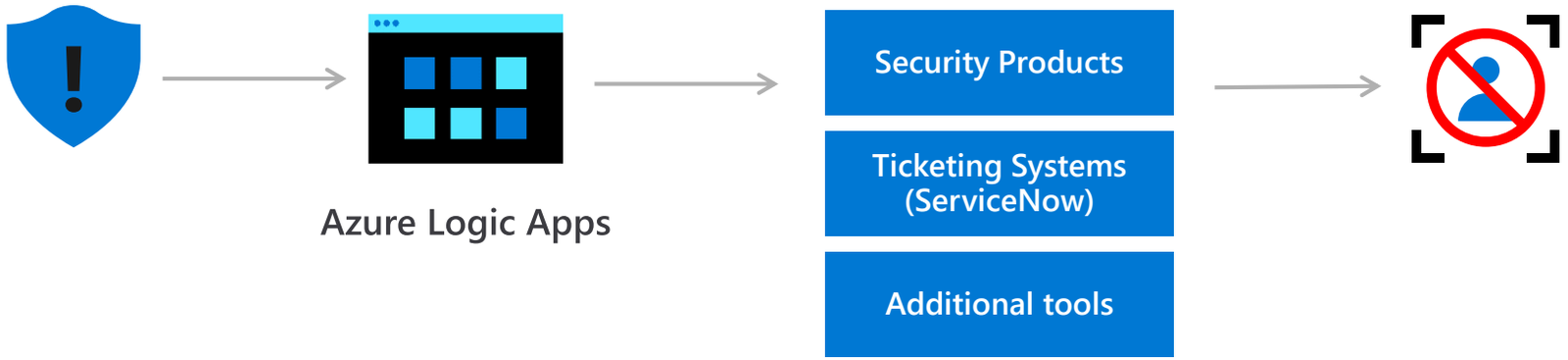
Visualize the entire attack and its impact

Hunt for suspicious activities using **pre-built queries and Azure Notebooks**



Respond rapidly with built-in orchestration and automation

Build automated and scalable playbooks that integrate across tools



Microsoft Azure

Thank you.